Application Note

Skype for Business 2015 using SIP trunk (TLS) to Cisco Unified Communications Manager Release 10.5.2 SU3

Table of Contents

Introduction 3
The following items were tested: 4
Listed below are the highlights of the integration issues: 4
Below are the key results: 4
Network Topology 5
Limitations 5
System Components 6
Hardware Requirements 6
Software Requirements 7
Features 8
Features Supported 8
Features Not Supported or Not Tested 8
Configuration 10
Configuring Sequence and Tasks: 10
Configuring the Skype for Business 11
Add Cisco UCM to Skype for Business Topology 11
Skype for Business Trunk Configuration 14
Skype for Business Route Configuration 19
Skype for Business Voice Policy and PSTN Usage Configuration 21
Skype for Business Dial Plan Configuration 22
Skype for Business Call Park Range Configuration 27
Skype for Business Global Media Bypass Configuration 28
Skype for Business User Configuration 29
Skype for Business Client Configuration 34
Configuring the Cisco Unified Communications Manager 36
Cisco Unified Communications Manager SIP Trunk Security Profile for Trunk to Skype for Business 36
Cisco Unified Communications Manager SIP Trunk Security Profile for Trunk to Unity Connection 37
Cisco Unified Communications Manager SIP Profile 38
Cisco Unified Communications Manager Media Resource Group 42
Cisco Unified Communications Manager Media Resource Group List 45
Cisco Unified Communications Manager Device Pool Configuration 47
Cisco Unified Communications Manager Region Configuration 49

Cisco Unified Communications Manager Normalization Script 49
Cisco Unified Communications Manager SIP Trunk to Skype for Business Configuration 57
Cisco Unified Communications Manager SIP Trunk to Cisco Unity Connection Configuration 63
Cisco Unified Communications Manager Route Group 69
Cisco Unified Communications Manager Route List 70
Cisco Unified Communications Manager SIP Route Pattern 71
Cisco Unified Communications Manager Voice Mail Configuration 72
Cisco Unified Communications Manager Route Pattern to Skype for Business Extensions 72
Cisco Unified Communications Manager Route Pattern to invoke Jabber client with Remote Destination configured as Skype for Business Extensions 74
Cisco Unified Communications Manager Route Pattern to Skype for Business Call Park range 76
Cisco Unified Communications Manager Route Pattern to Unity Connection Voice Mail 78
Cisco UCM Extent and Connect 79
Cisco UCM UC service Configuration 79
Cisco UCM service Profile Configuration 81
Cisco Unified CM IM Presence – CCMCIP Profile Configuration 83
Cisco UCM – SIP trunk to Cisco IM&Presence Trunk Configuration 84
Cisco UCM end user configuration 88
Remote Destination Configuration 92
Cisco UCM CTI Remote Device Configuration 93
Cisco Unity Connection 97
Cisco Unity Connection Telephony Integration – Add Phone System 97
Cisco Unity Connection Telephony Integration – Add Port Group 97
Cisco Unity Connection Telephony Integration – Add Ports 99
Cisco Unity Connection User Configuration 100
Acronyms 103

Introduction

This document describes the steps and configurations necessary for Cisco Unified Communications Manager (Cisco UCM) release 10.5.2 to interoperate with the Skype for Business 2015 on TLS using the following configuration:

On the Cisco UCM: PRACK Enabled and Early Offer SIP Profile.

On the Skype for Business: Media Bypass Disabled, Encryption support level Optional

The following items were tested:

- Basic call between the two systems and verification of voice path, using SIP phones on Cisco, and SFB client on the Skype for Business (Refer to limitation section for more info)
- CLIP/CLIR/CNIP/CNIR features: calling party Name and number delivery (allowed and restricted) (Refer to limitation section for more info)
- COLP/CONP/COLR/CONR features: connected Name and number delivery (allowed and restricted) (Refer to limitation section for more info)
- Call transfer: attended and early attended (Refer to limitation section for more info)
- Alerting Name Identification (Refer to limitation section for more info)
- Call forwarding: call forward unconditional(CFU), call forward busy (CFB), and call forward no answer (CFNA)
- Hold and resume with music on hold
- Three-way conferencing (Refer to limitation section for more info)
- Voice messaging and MWI activation-deactivation (Refer to limitation section for more info)
- Extend and Connect (Refer to limitation section for more info)
- Call Park (Refer to limitation section for more info)

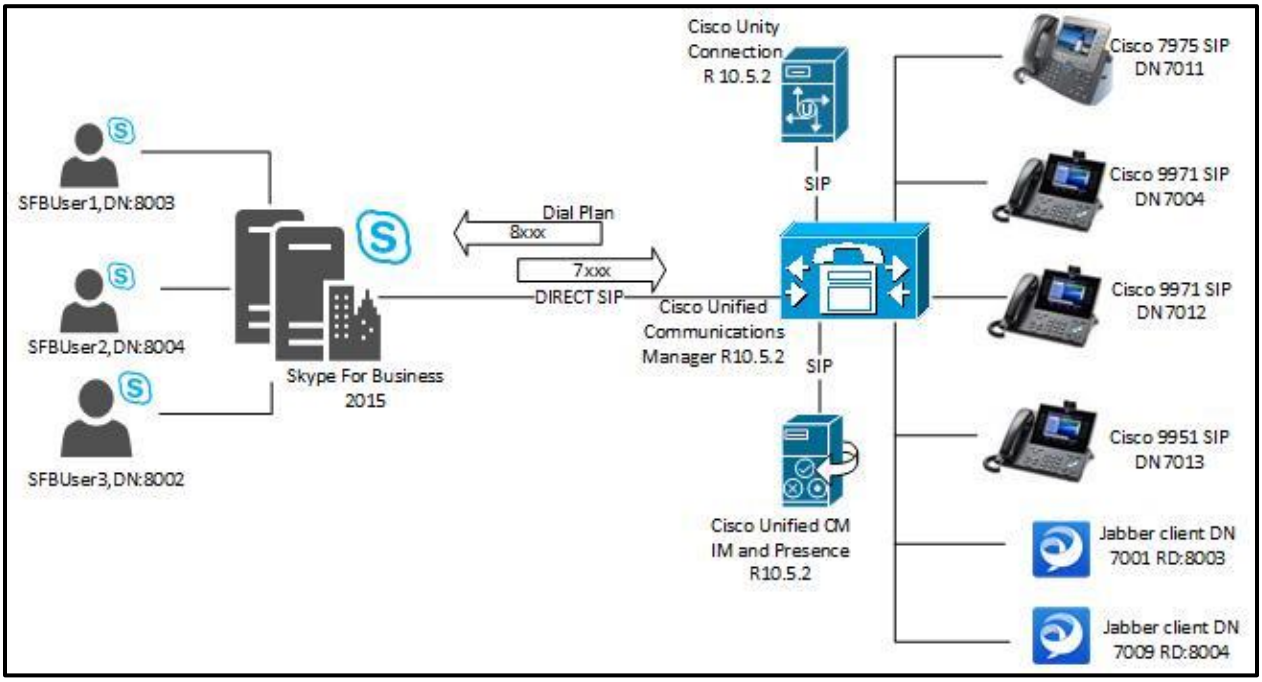
Listed below are the highlights of the integration issues:

- Basic calls work from Cisco UCM to Skype for Business and vice versa. Testing has been done with Cisco SIP phones only as SCCP phones do not support 80-bit crypto required by Skype for Business.
- Caller name and number is not updated correctly for basic calls and in the attended and early-attended transfer scenarios.
- Caller ID is updated to “Unknown Number” on Cisco UCM SIP phones in transfer scenarios when a Skype for Business user initiates the transfer.
- Alerting name updates do not occur on Skype for Business.
- Video calls between the Cisco UCM and Skype for Business users were not tested.

Below are the key results:

- Basic call, call transfer, call forwarding, conference call, and hold and resume tested successfully with a few caveats and limitations.
- Centralized voicemail, using Unity Connection server integrated with Cisco UCM via SIP is used for testing. This voicemail solution can provide centralized voicemail services, supporting both Skype for Business and Cisco end-users.

Network Topology



Limitations

These are the known limitations, caveats, or integration issues:

- Skype for Business and Cisco UCM do not support overlap dialing modes on their SIP endpoints.
- Skype for Business does not support alerting name updates.
- Skype for Business does not update the caller ID (connected Name) for a basic or privacy enabled call from the Cisco UCM. Therefore, only the connected party number is displayed on the Cisco UCM Phone.
- Skype for Business does not consider Privacy ID which is being sent by Cisco UCM during 180 Ringing or 200 OK when Connected Name/ID is resticted on Cisco UCM. Consequently, Skype for Business does not update Connected Party display as Private.
- Skype for Business does not update the CLID in transfer/conference scenarios. After the transfer/conference is complete, Cisco UCM sends mid call INVITE and UPDATE messages that contain PAI and RPI. However, Skype for Business does not update this information on its clients.
- In a transfer scenario, when Skype for Business initiates the call transfer, the caller ID of the initial Cisco UCM calling endpoint (transferee) is updated to “Unknown Number” if it is a SIP phone.
- When there is a call leg between two Skype For Business Users, of which either one of the users or both the users are Extend and Connect devices, there is one-way audio. This is noticed during the initiation of some transfer and conference test cases. However when transfer or conference is completed, there is no one-way audio issue noticed and all the parties in the call could hear each other.

- Cisco UCM user is not able to complete an attended transfer when its both the call legs are established with Skype For Business Users that are Extend & Connect devices.
- In a call park scenario, when a Skype for Business client initiates the call park, the Cisco UCM endpoint that retrieves the parked call has its caller ID updated to "Unknown Number".
- Cisco UCM user parks a call with Skype For Business user. When another Skype For Business user retrieves that call, there is one-way audio. The Skype for Business user, who is retrieved from parking, could not hear the other user.
- Skype for Business does not send PAI by default i.e. when restriction is not enabled. This fails to initiate the Jabber client for call control. The incoming call to a Cisco UCM endpoint is therefore like a regular call without remote destination configuration.
    - This is currently a known issue on the Cisco UCM and is addressed by *"CSCuz48313 Tel URI | PAI support in CUCM*".
    - As a workaround, the RD is configured with a "+" prefix and a route pattern to route a DN with a "+' preix is also added. (Refer Cisco UCM configuration section - *Cisco Unified Communications Manager Route Pattern to invoke Jabber client with Remote Destination configured as Skype for Business Extensions*.
- Skype for Business does not support MWI notification from Cisco Unity Connection. It responds with a "405 Method Not Allowed" to a NOTIFY Message from the Cisco UCM that has MWI information.
- In Multiple Call Forwarding scenario between Skype for Business Users and Cisco UCM Users, wherein both originator and terminator being Skype for Business Users, originator does not display the Caller ID of terminator.
- In a call forwarding scenario that involves multiple call forwards and a loop that terminates on a Cisco UCM or Skype for Business user, the calling party (Skype for Business client or Cisco UCM endpoint) hears a re-order tone when it calls the user on which the loop is formed.
- When Cisco UCM user initiates MOH, MOH is RTP. Pad-lock symbol on the phone disappears.
- When Cisco UCM User completes the conference, the audio is on RTP. Pad-lock symbol on the Cisco phone disappears. Audio is on RTP regardless of whether Software based conferencing is used or IOS based conferencing is.

System Components

Hardware Requirements

The following hardware is required:

- Cisco UCS-C240-M3S VMWare Host
- Cisco 7960,7965 ,7975, 9951, and 9971 IP phones

Software Requirements

The following software is required:

- Cisco UCSC-C240-M3S VMware vSphere Image Profile: ESXi-5.5.0-1331820-standard
- Cisco Unified Communications Manager release 10.5.2.13900-12
- Cisco Unified Communications Manager IM & P release 10.5.2.13900-12
- Cisco Unity Connection release 10.5.2.13900-12
- Cisco Jabber 11.6.0 Build 35037
- Skype for Business 2015 6.0.9319.0
- Skype for Business Client version : 15.0.4841.1000

Features

This section lists supported and unsupported features. No deviation from the configuration presented in this document shall be supported by Cisco. Please see the Limitations section for more information.

Features Supported

- CLIP—calling line (number) identification presentation
- CLIR—calling line (number) identification restriction
- CNIP—calling Name identification presentation
- CNIR—calling Name identification restriction
- Alerting Name
- Attended call transfer
- Early attended call transfer
- CFU—call forwarding unconditional
- CFB—call forwarding busy
- CFNA—call forwarding no answer
- COLP—connected line (number) identification presentation
- COLR—connected line (number) identification restriction
- CONP—connected Name identification presentation
- CONR—connected Name identification restriction
- Hold and resume
- Conference call
- MWI—Message Waiting Indicator (only for Cisco Endpoints)
- Audio Codec Preference List
- Call Park/Pickup(see limitation section)
- Extend and Connect
- Shared Line on Cisco Endpoints

Features Not Supported or Not Tested

- Call completion (callback, automatic callback)
- Shared Line on Skype for Business
- Message Waiting Indicator on Skype for Business Endpoints
- Blind transfer

- Video calls
- Scenarios that required 3 PBXs.
- Scenarios involving Non-SIP interfaces.
- Scenarios involving Cisco UCM SCCP Phones

Configuration

The goal of this guide is to provide an overview of the integration between Cisco Unified Communication Manager and Skype for Business. The deployment will interconnect the UC systems using SIP. No PSTN connectivity has been tested with this integration. The following sections provide the required configurations for a successful integration.

Configuring Sequence and Tasks:

Skype for Business:

- Add Cisco UCM to Skype for Business Topology
- Trunk Configuration
- Route Configuration
- Voice Policy and PSTN Usage Configuration
- Dial Plan Configuration
- Call Park range Configuration
- Media Bypass Configuration
- User Configuration
- Client Configuration

Cisco Unified Communications Manager:

- SIP trunk security profile
- SIP profile
- Media resource group and media resource group list
- Assign media resource group list (MRGL) in the default device pool
- Region configuration
- Normalization script
- SIP trunk to Skype for Business
- SIP Trunk to Cisco Unity Connection
- Assign User in Cisco Unity Connection
- SIP and SCCP phones device configuration
- Route Group, Route List and SIP Route Pattern
- Voice Mail
- Route pattern to Skype for Business, Unity Connection and Skype for Business call park range
- Extend and Connect Feature and User configuration

Cisco Unity Connection:

- Cisco Unity Connection Telephony Integration
- Cisco Unity Connection User Configuration

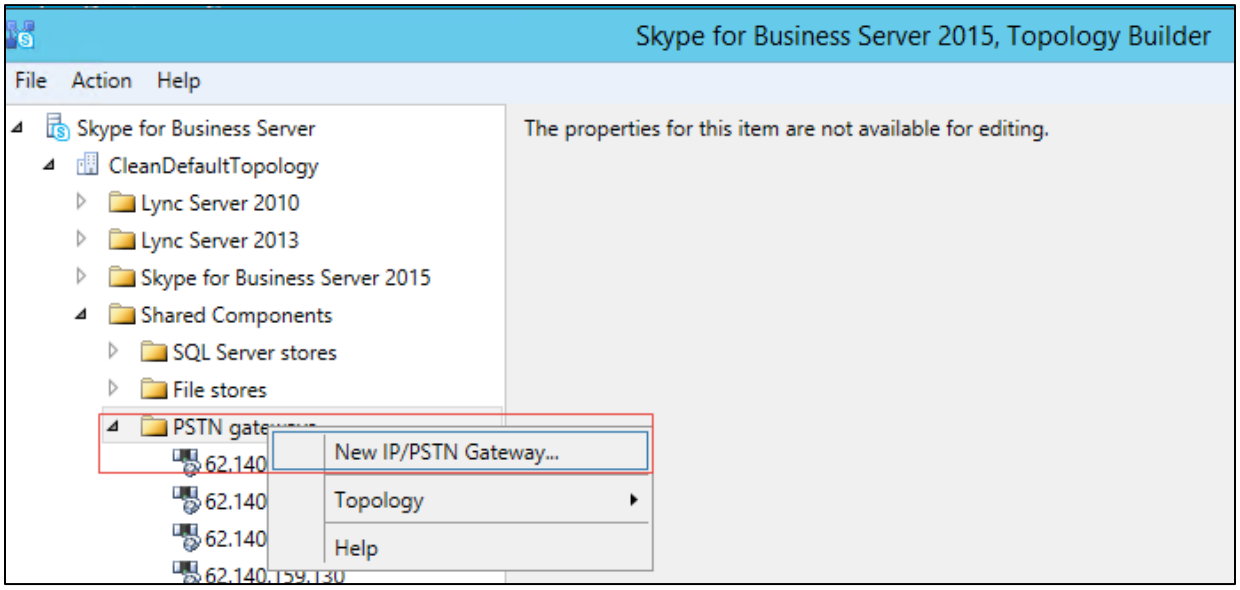
Configuring the Skype for Business

Add Cisco UCM to Skype for Business Topology

Run the Skype for Business 2015 Topology Builder as a user in the CSAdministrator group.

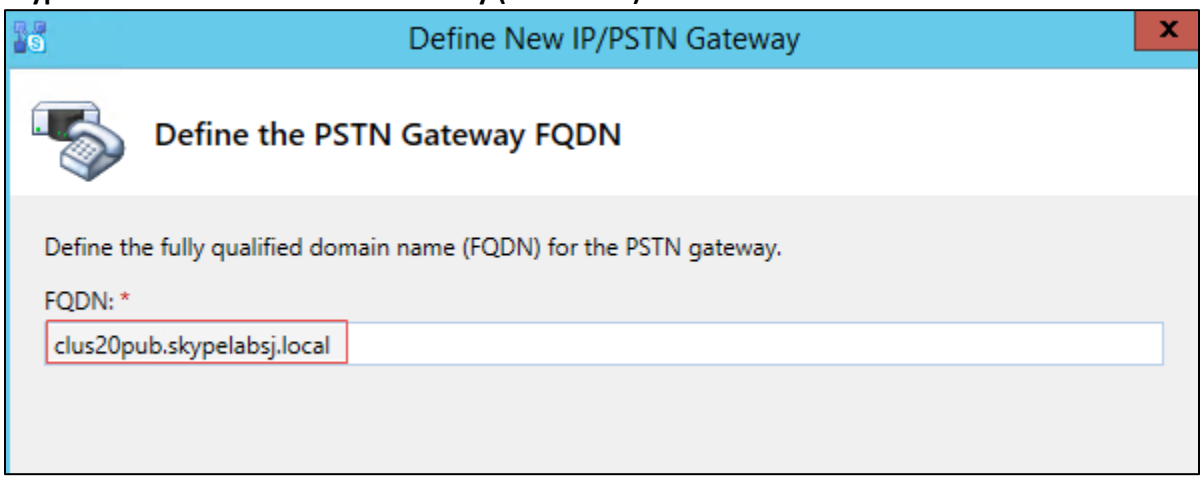
Navigation: Skype for Business Server→CleanDefaultTopology→Shared Components→PSTN gateways

Right click and select "New IP/PSTN Gateway"



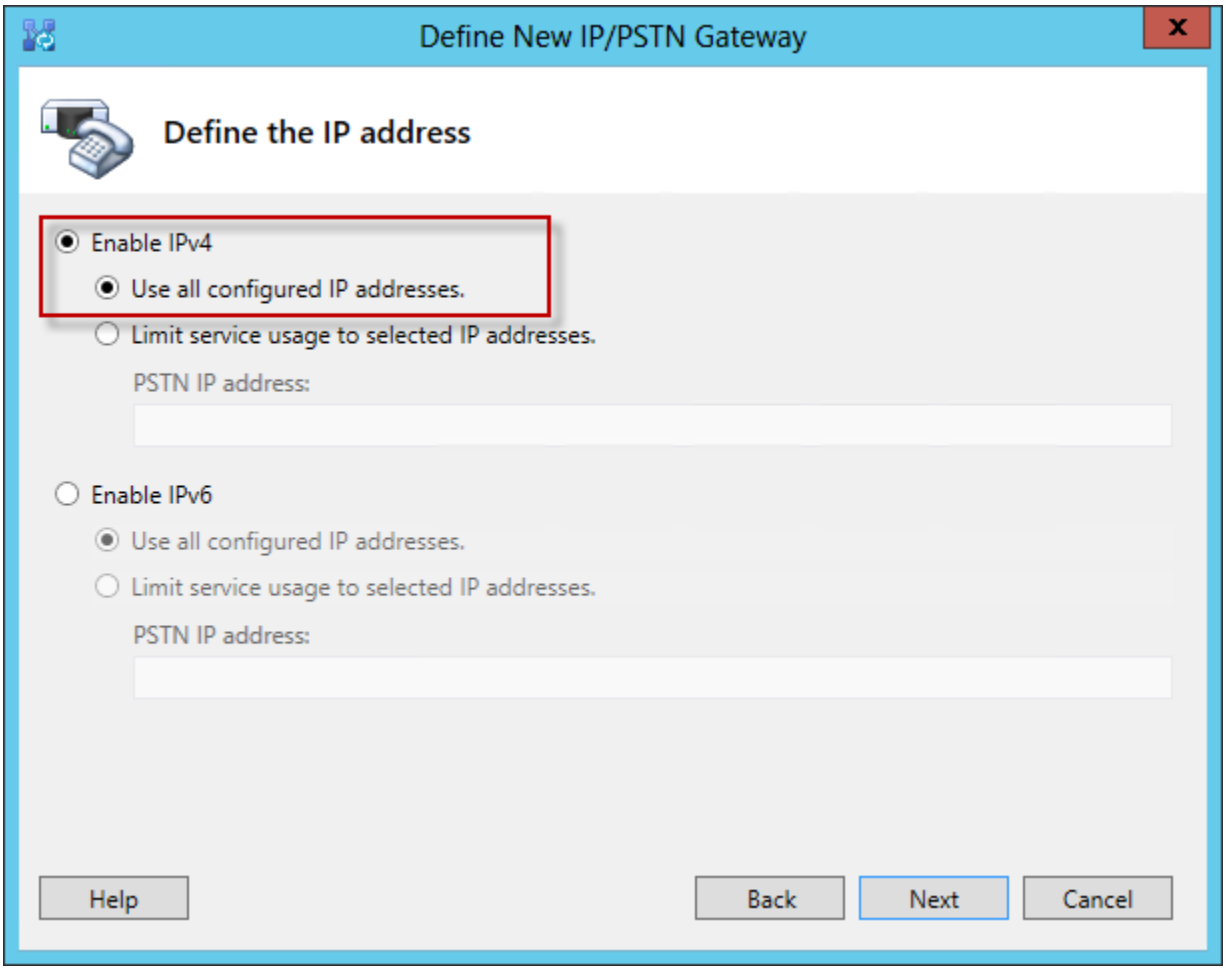
Set FQDN = <FQDN of the Cisco UCM>– clus20pub.skypelabsj.local is used in this test.
Click Next.

Skype for Business – Add PSTN Gateway (Continued)



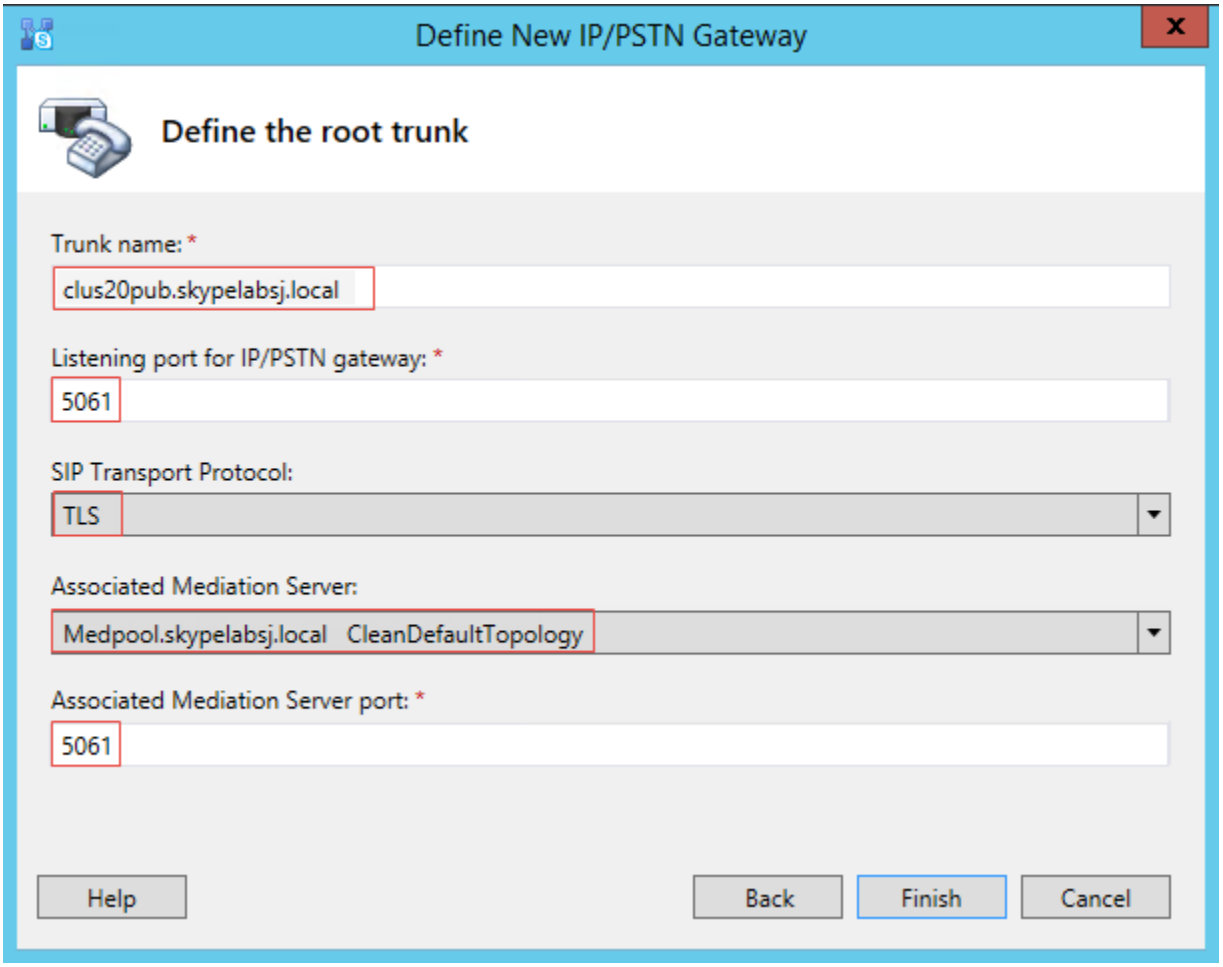
Check the Enable IPv4 and Use all configured IP addresses radio button
Click Next.

Skype for Business – Add PSTN Gateway (Continued)



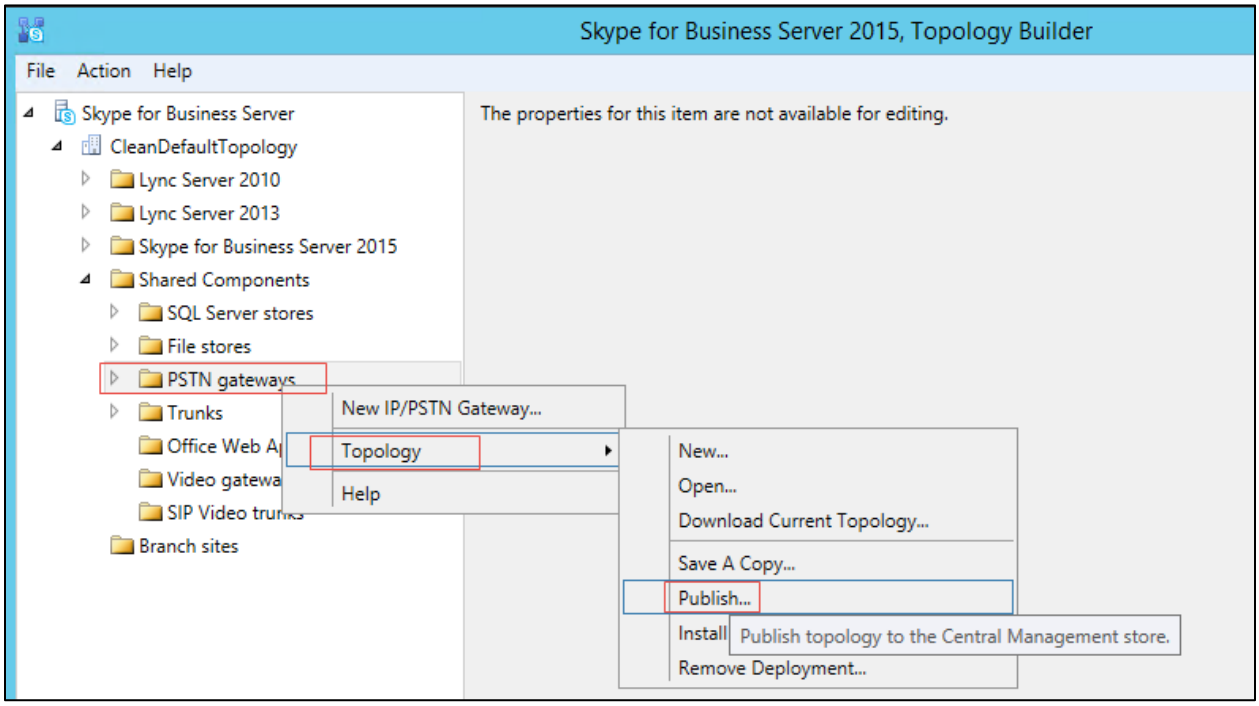
Set Trunk Name = FQDN of the Cisco UCM – clus20pub.skypelabsj.local is used for this test
Set **Listening port for IP/PSTN gateway =** The **Listening port** should match the **Incoming Port** setting in the CISCO UCM's **SIP Trunk Security Profile – 5061** is used for this test
Set **SIP Transport Protocol** = TLS
Set **Associate Mediation Server**: Assign this PSTN gateway to the Front End co-located mediation server – Medpool.skypelabsj.local is used for this test.
Click Finish.

Skype for Business – Add PSTN Gateway (Continued)



Publish the topology so these new configurations take effect.

Skype for Business – Add PSTN Gateway (Continued)

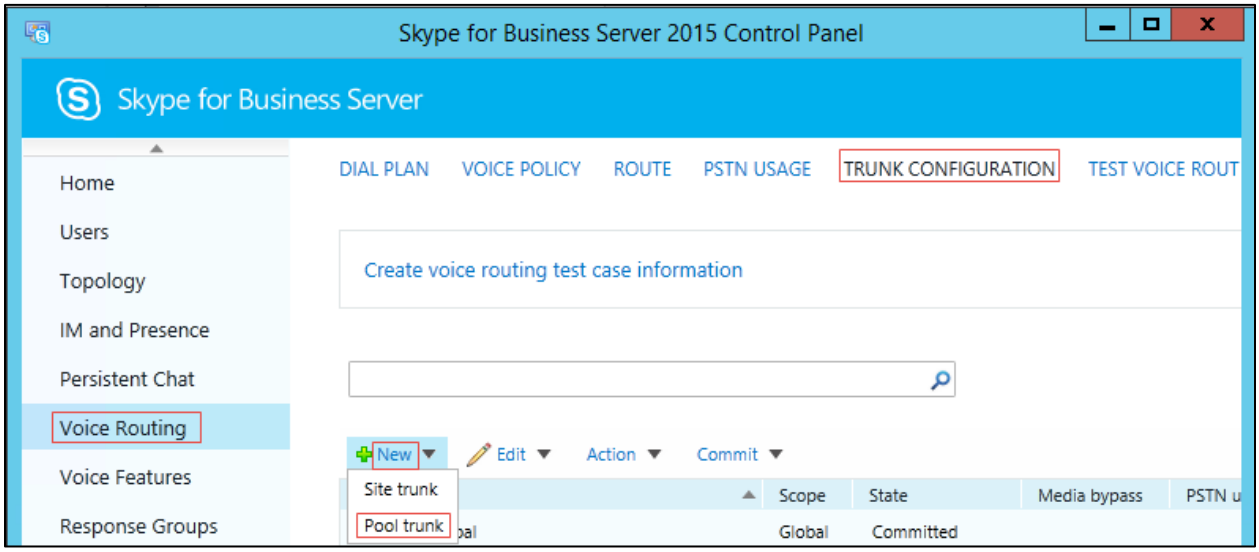


Skype for Business Trunk Configuration

Open the Skype for Business 2015 Control Panel.

Navigation: Voice Routing -> Trunk Configuration

Select New →Pool Trunk



Set Service = Trunk to Cisco UCM that was created earlier as a PSTN gateway in the topology builder – clus20pub.skypelabsj.local is used for the test.

Set **Maximum early dialogs supported** = 20

Set **Encryption support level =** Optional

Set **Refer Support =** Enable sending refer to the gateway

Uncheck **Enable media bypass**

Check **Centralized media processing**

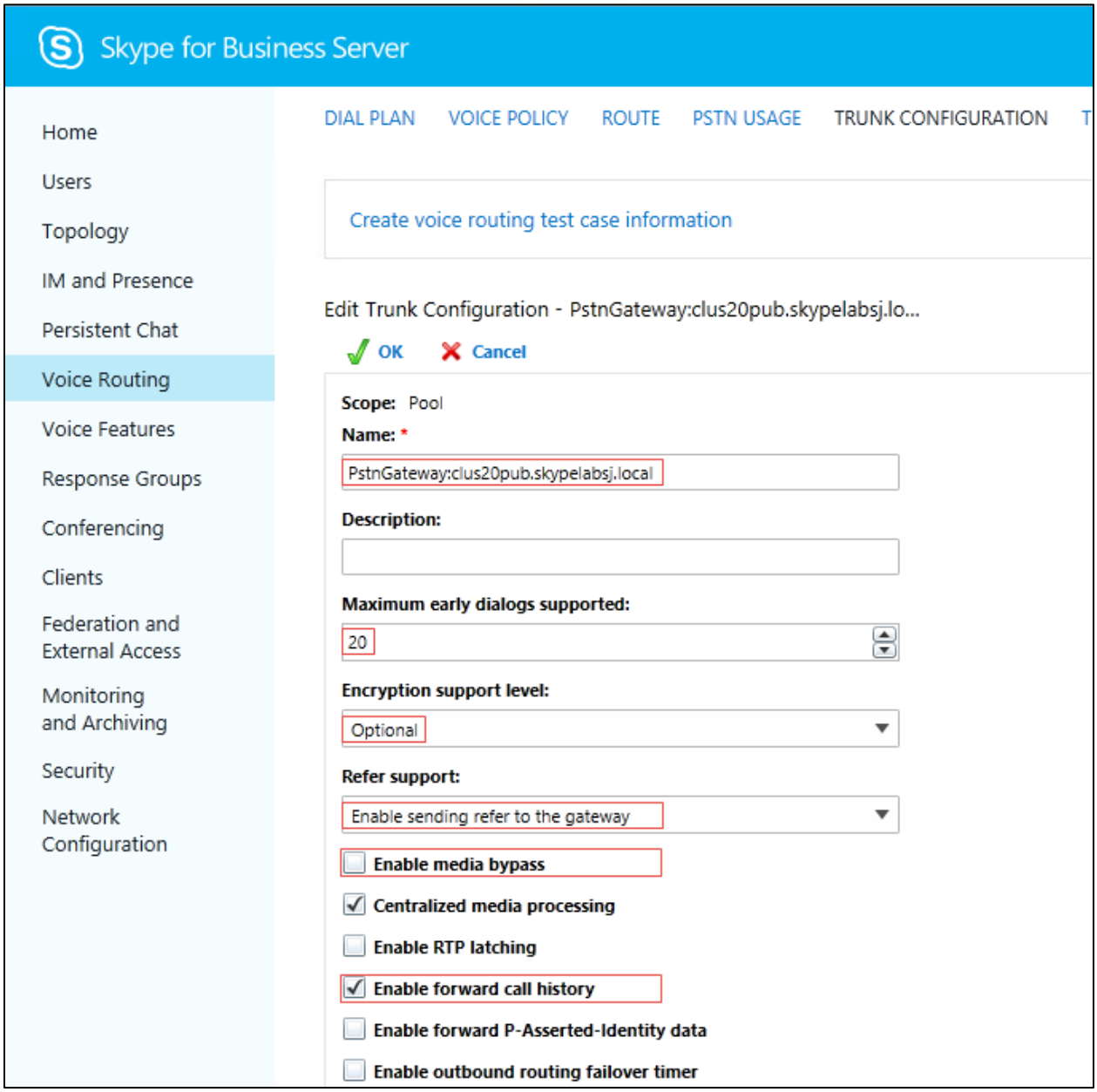
Uncheck **Enable RTP latching**

Check **Enable forward call history**

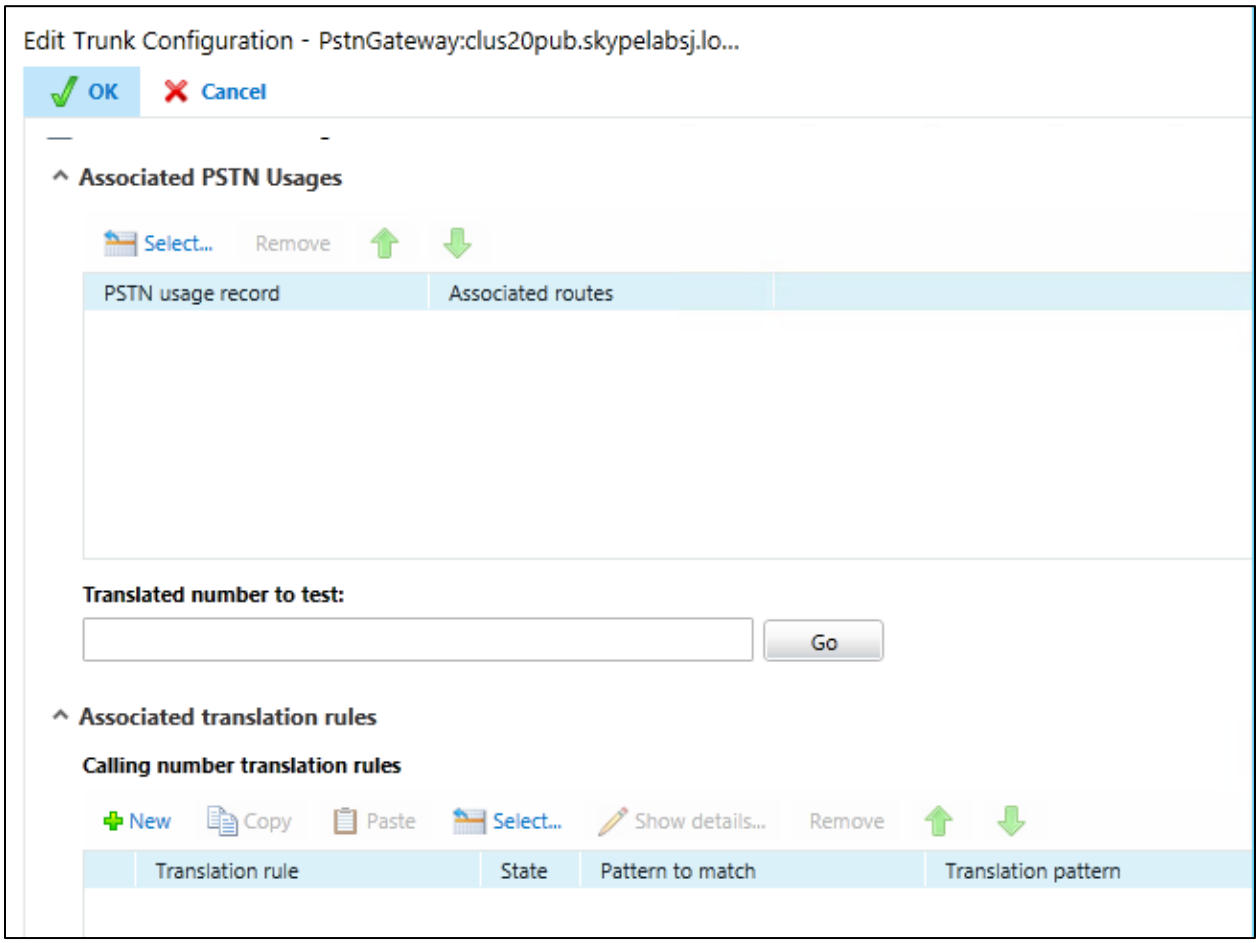
Uncheck **Enable forward P-Asserted-Identity data*** [Note: this is checked when test scenarios that involve restrict ID need to be executed]

Uncheck **Enable outbound routing failover timer**

Skype for Business –Trunk Configuration (Continued)

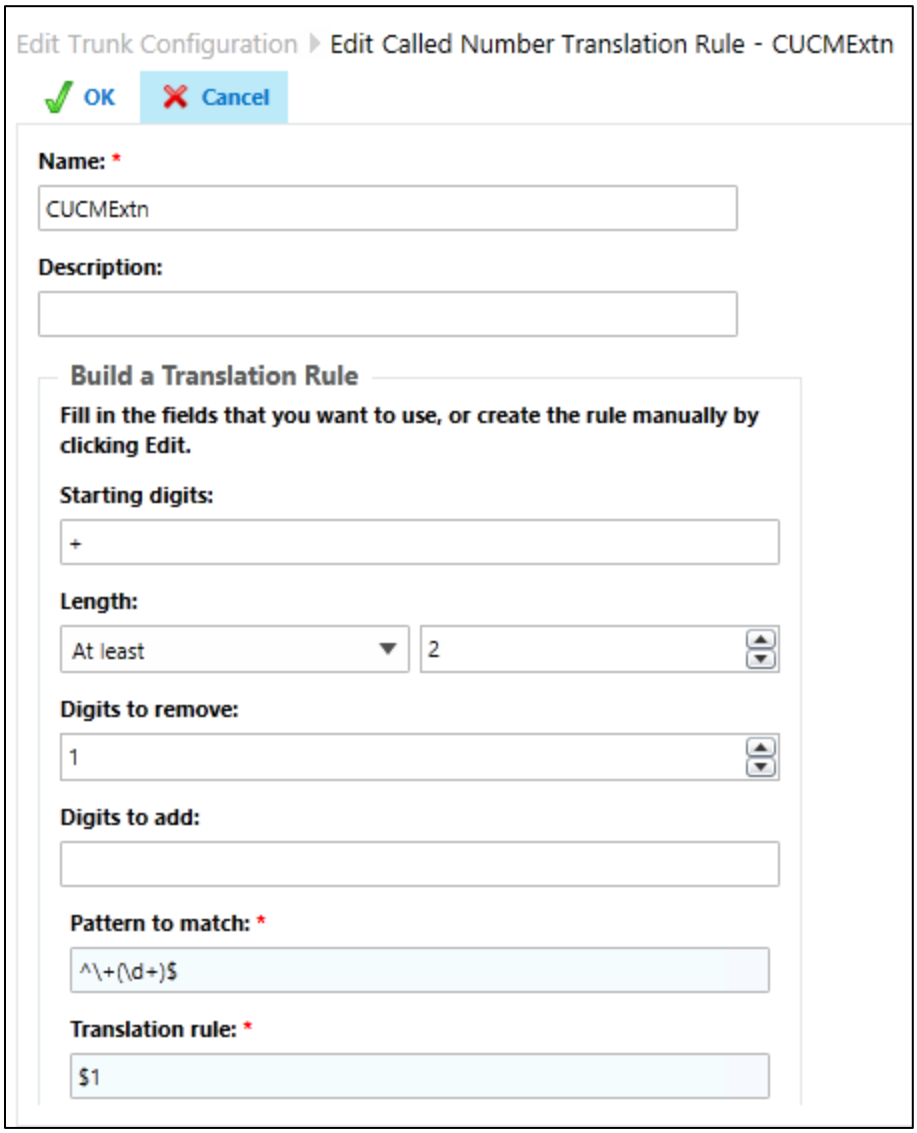


Skype for Business –Trunk Configuration (Continued)

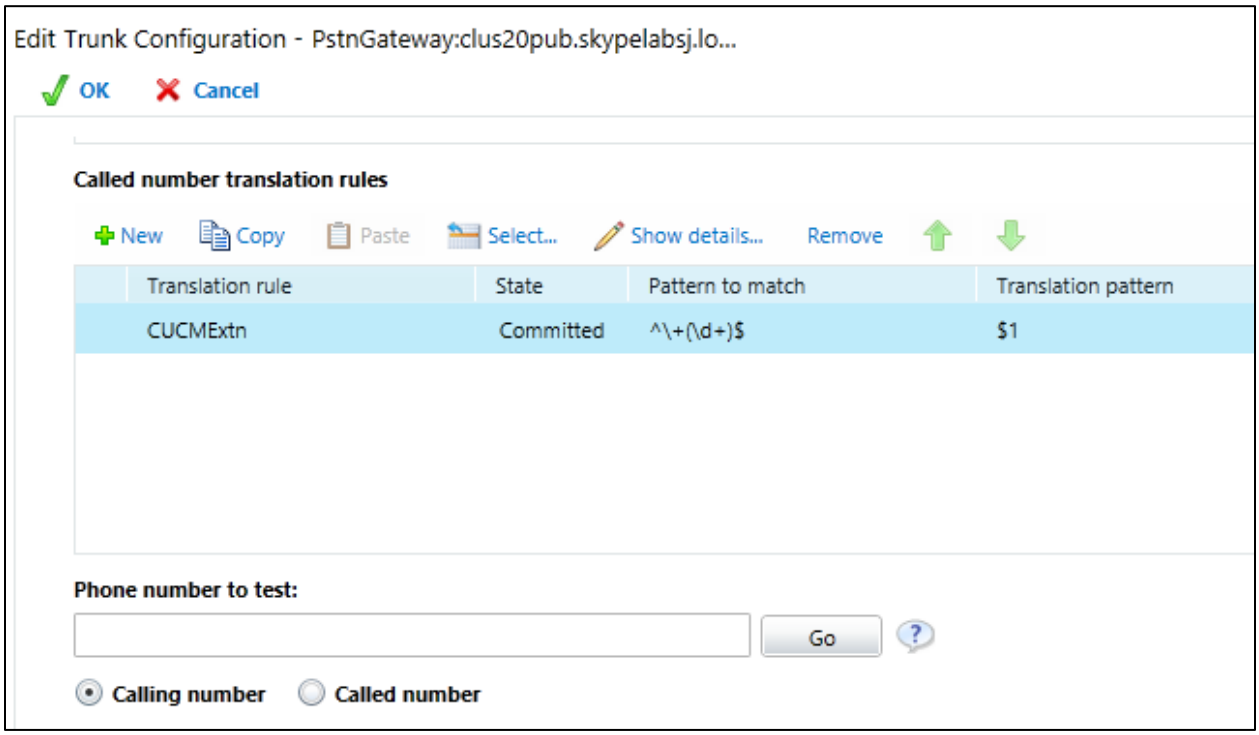


Add a Translation rule under Called number translation rules – **CUCMExtn** was created in this test.
This is used to remove the "+" that is added by Skype for Business during a transfer to a Cisco UCM extension.
If Skype for Business attempts a transfer to a Cisco UCM extension without this rule, the transfer fails because the extension is not recognized by Cisco UCM.

Skype for Business –Trunk Configuration- Translation Rule



Skype for Business –Trunk Configuration (Continued)



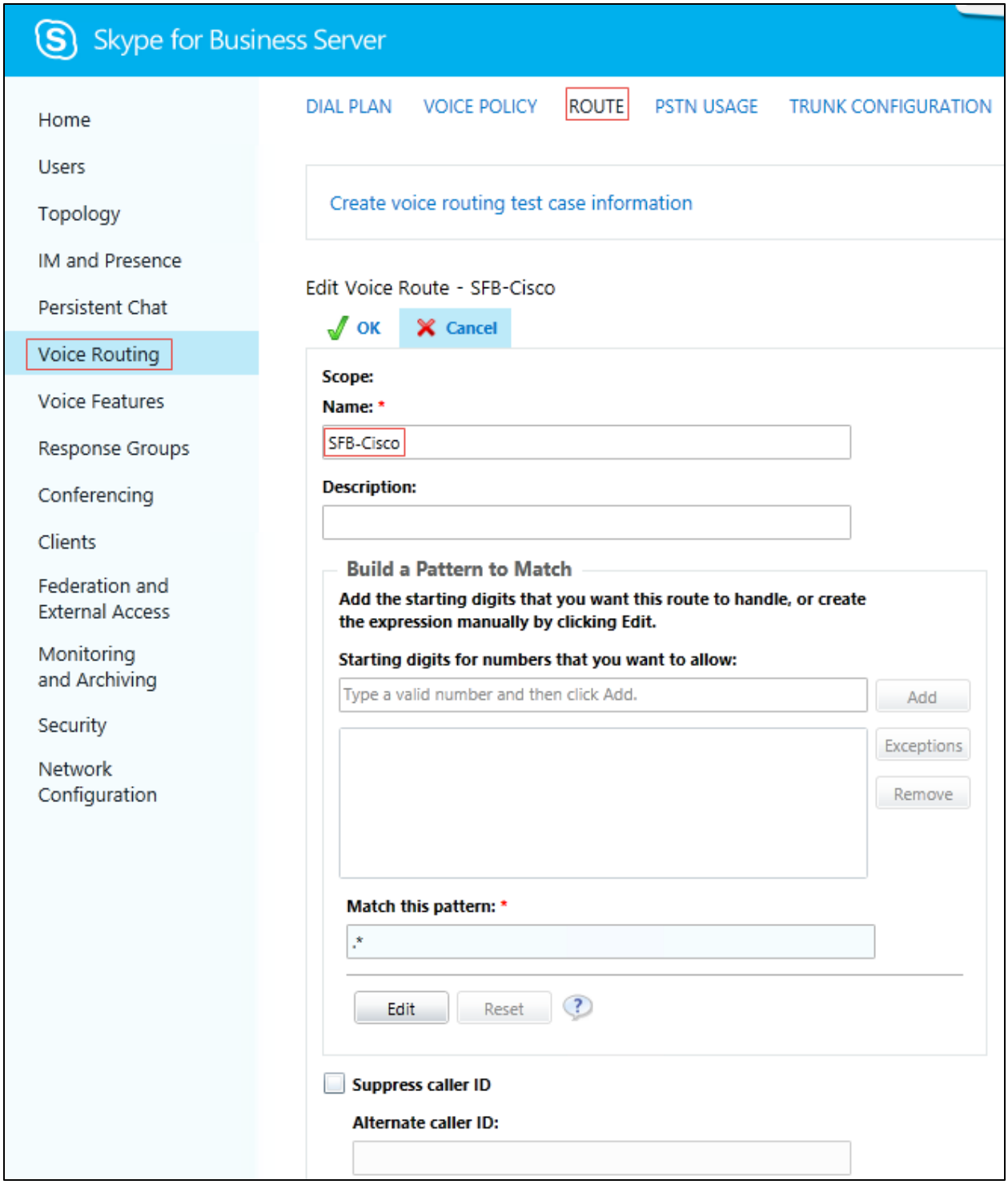
Skype for Business Route Configuration

Navigation: Voice Routing -> Route

Click New

Set Name = enter a name to identify this Route. SFB-Cisco is used for this test.

Add Associated trunks = select the trunk configured earlier – PstnGateway:clus20pub.skypelabsj.local



Skype for Business Voice Policy and PSTN Usage Configuration

Navigation: Voice Routing -> Voice Policy

Click New

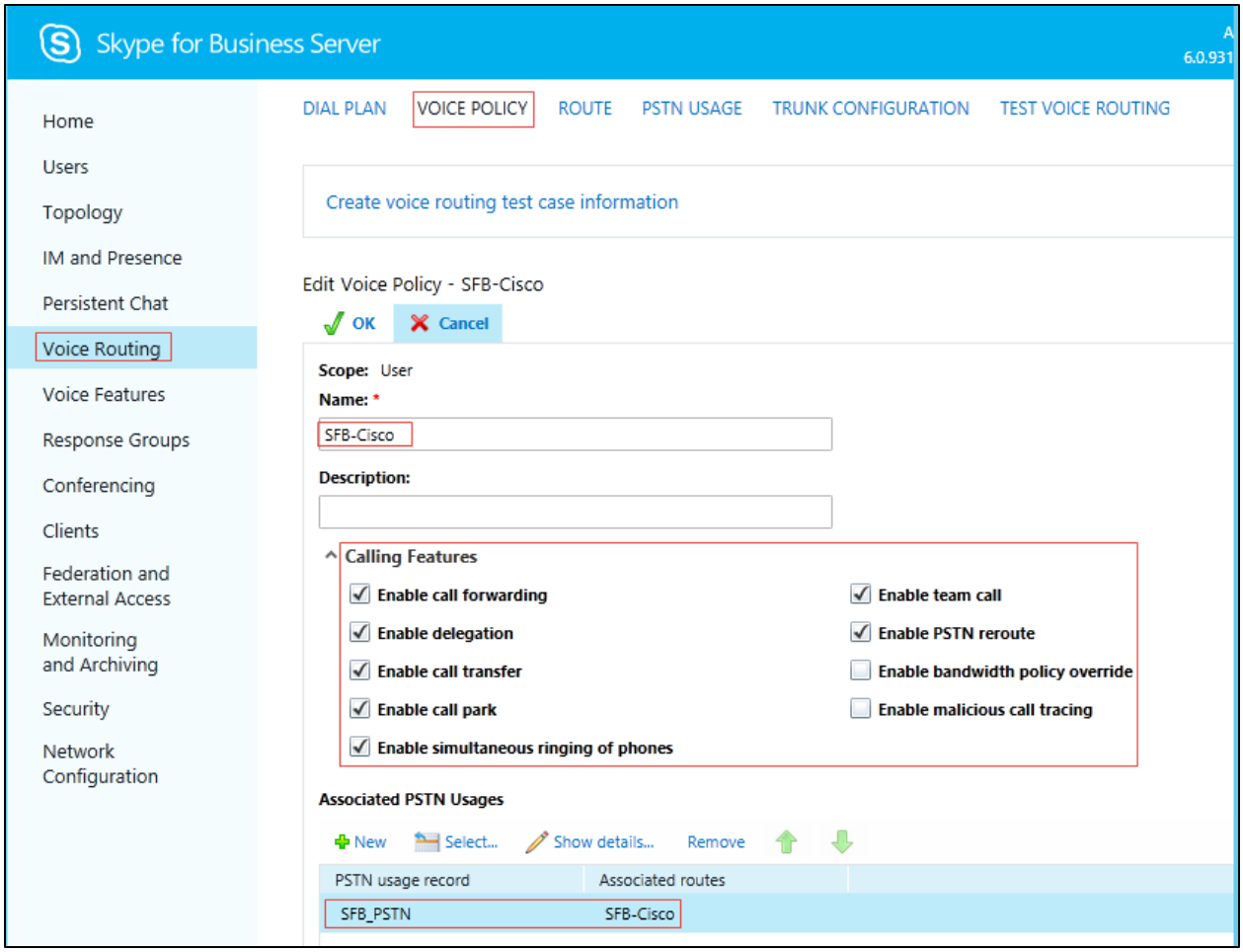
Set Name = enter a name to identify this voice policy – SFB-Cisco is used in this test.

Set Calling Features:

- Check Enable call forwarding
- Check Enable delegation
- Check Enable call transfer
- Check Enable call park
- Check Enable simultaneous ringing of phones
- Check Enable team call
- Check Enable PSTN reroute
- Uncheck Enable bandwidth policy override
- Uncheck Enable malicious call tracing

Set Associated PSTN usages:

- Click New
- Set Name: enter a name to identify this PSTN Usage record – SFB_PSTN is used in the test.
- Set Associated Routes = select the route created earlier= SFB-Cisco



Skype for Business Dial Plan Configuration

Navigation: Voice Routing-> Dial Plan

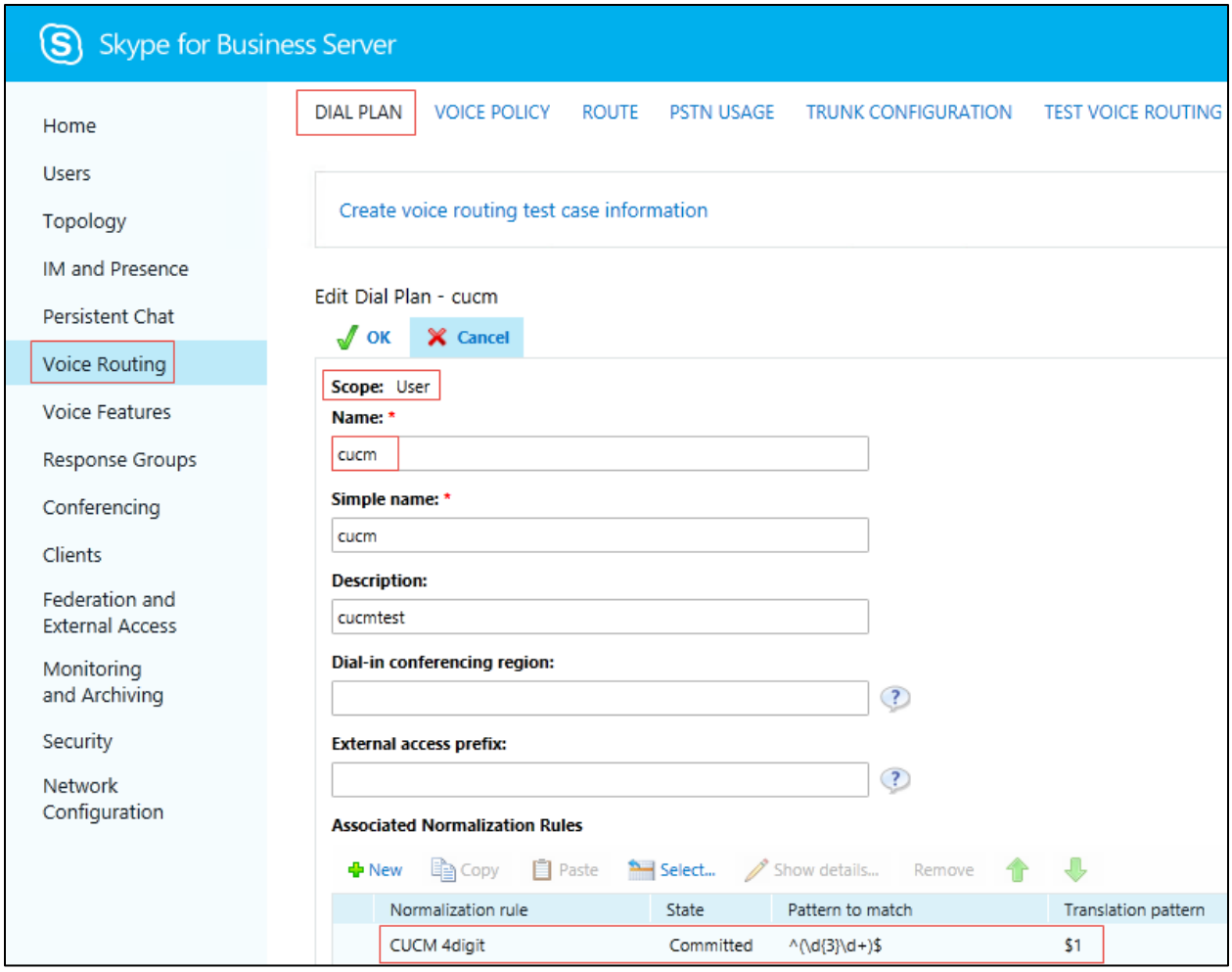
Add a new User dial plan and a new Pool dial plan.

User dial plan:

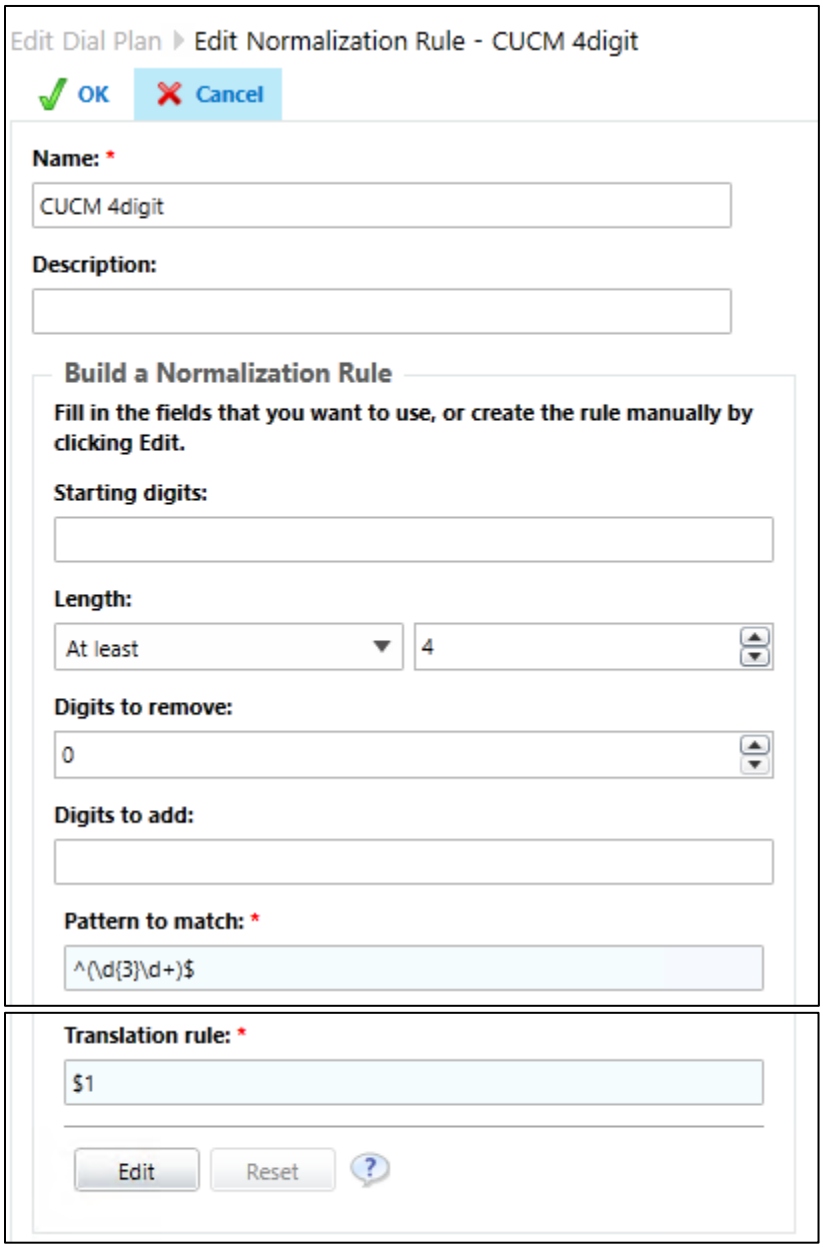
Set Name = enter text to identify this dial plan – *cucm* is used in this test.

A user dial plan with a normalization rule was configured for this test:

- CUCM 4 Digit: To reach the 4 digit extensions from Cisco UCM – This allows 4 digits to be dialed and not undergo any normalization.



Skype for Business – User Dial Plan-Normalization Rule



Pool dial plan:

Select Service: PstnGateway:clus20pub.skypelabsj.local is selected

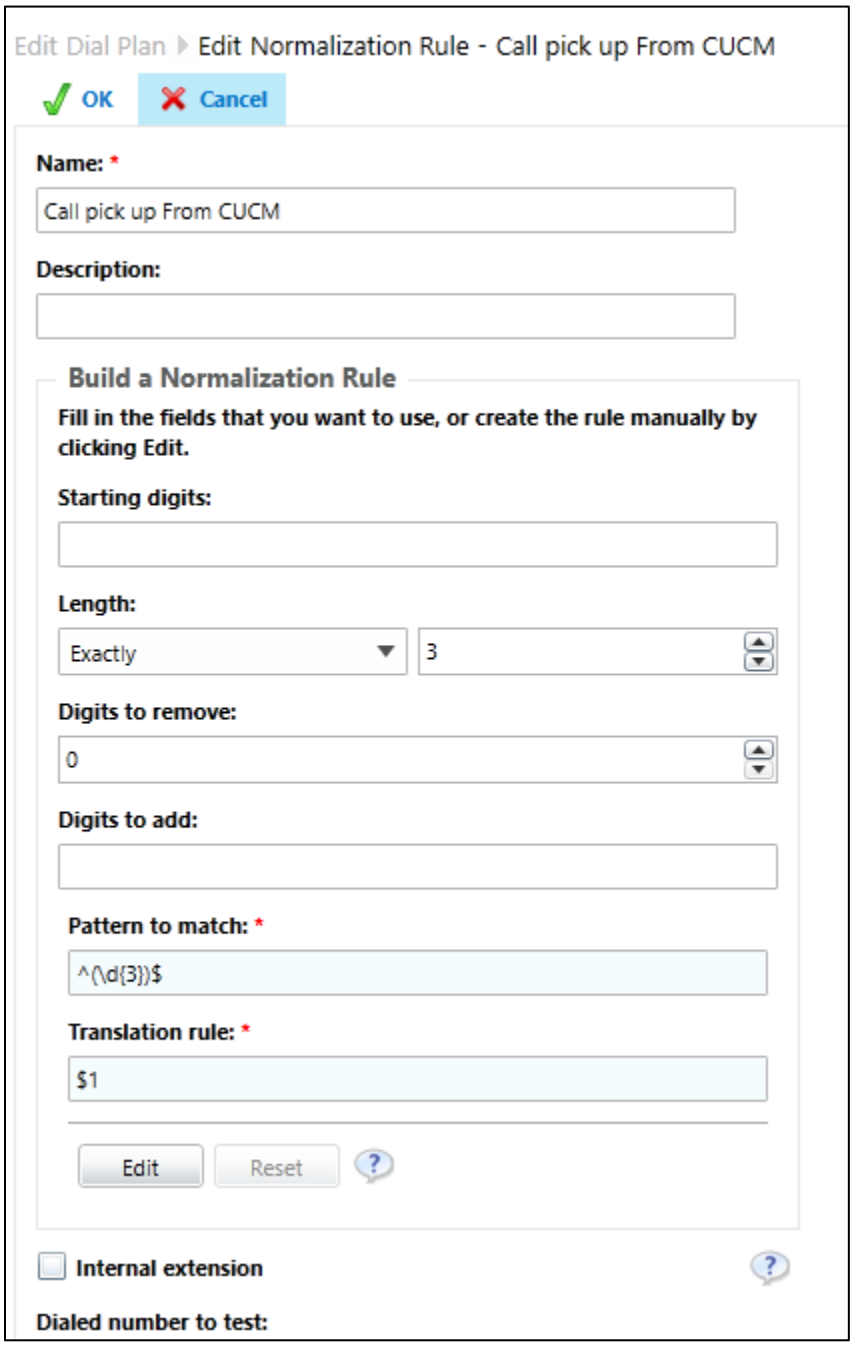
Set Simple Name= enter text to identify this pool dial plan. PstnGateway_clus20pub.skypelabsj.local is used in this test

Associated Normalization Rules→New

Set Name: enter text to identify this rule – Call pick up From CUCM was created in this test

This is to accept the call park range dialed by Cisco UCM users to retrieve a call parked by the Skype for Business client.

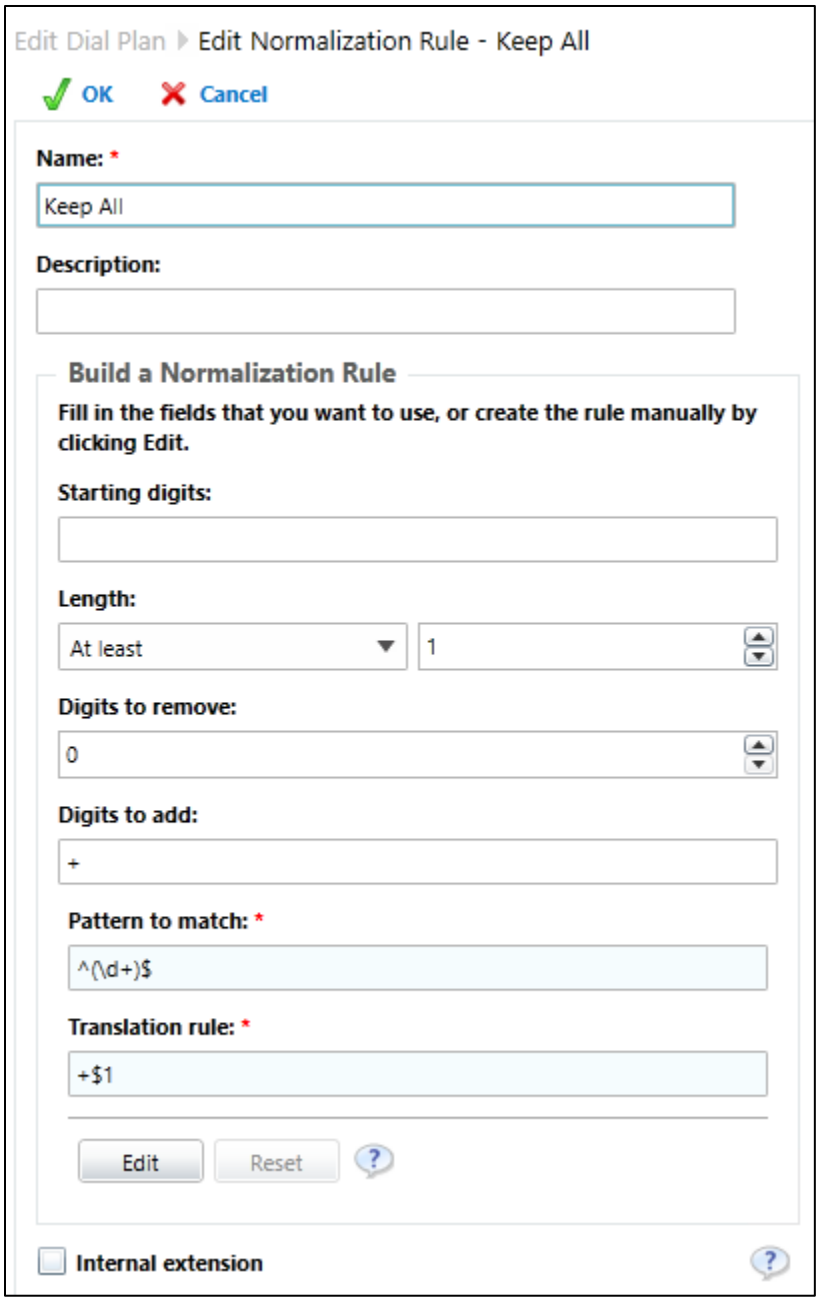
Skype for Business – Pool Dial Plan-Normalization Rule 1



Add another normalization rule as below:

This is used by the client to dial out to internal extensions and to the external PBX i.e. Cisco UCM

Skype for Business – Pool Dial Plan-Normalization Rule 2



Skype for Business Call Park Range Configuration

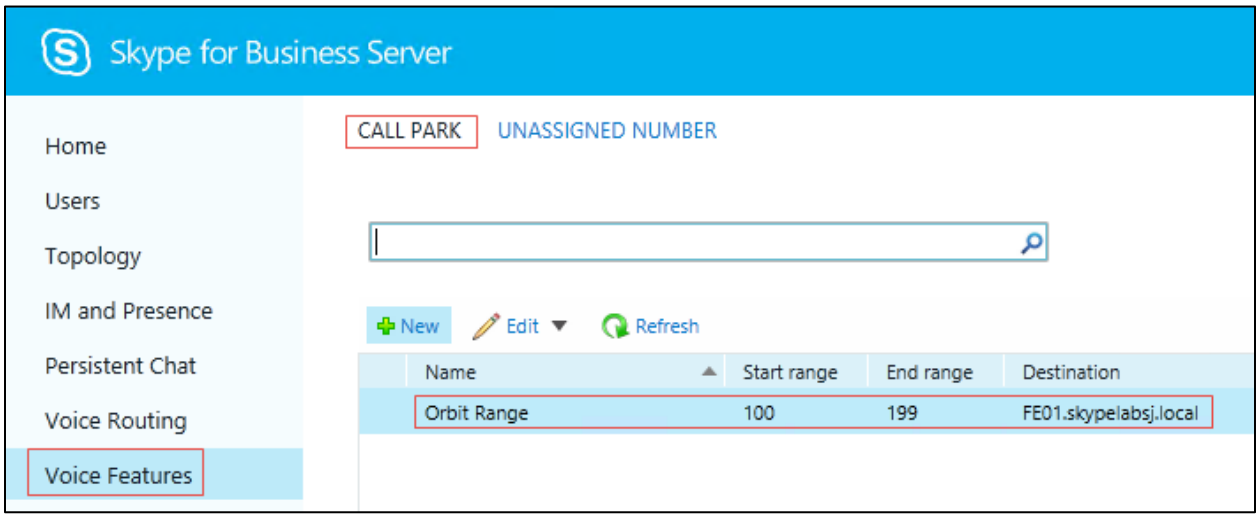
Navigation: Voice Features -> Call Park

Click New.

Set Name = enter text to identify this call park range – Orbit range is used in the test.

Set Number Range = 100 to 199 is used in the test.

Set FQDN of destination server= select the desired server - FE01.skypelabsj.local is used in the test



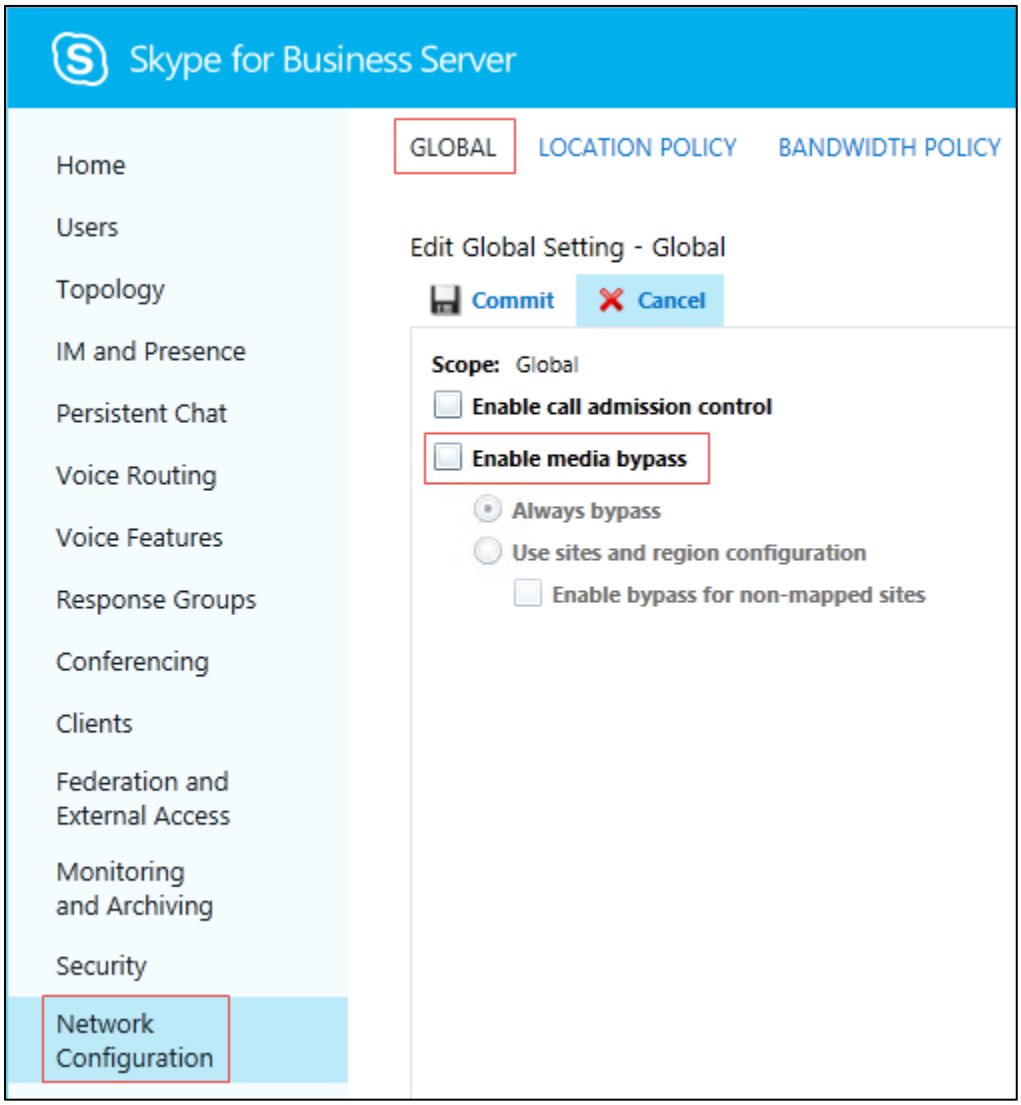
Skype for Business Global Media Bypass Configuration

Navigation: Network Configuration -> Global

Edit Global Setting –

- Uncheck Enable media bypass

Commit the configuration.

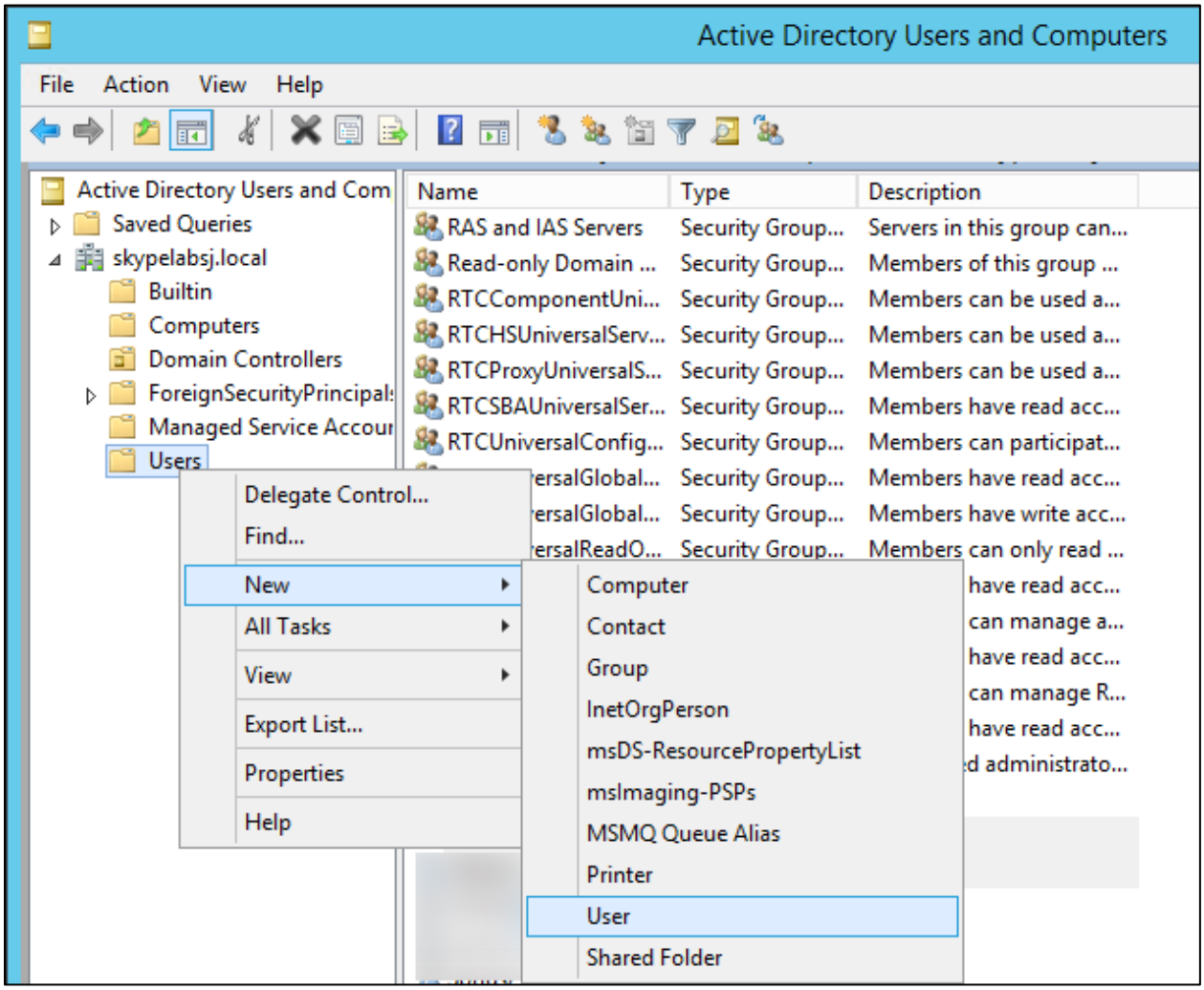


Skype for Business User Configuration

Login to the Skype for Business Active Directory

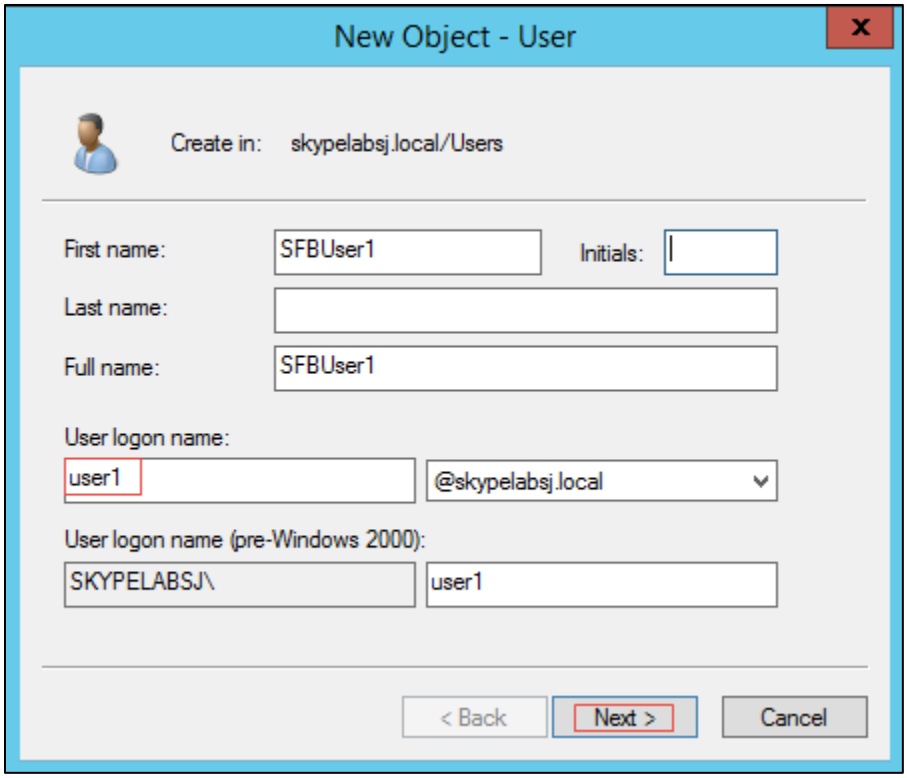
Navigation: Active Directory Users and Computers →Users

Add a New User

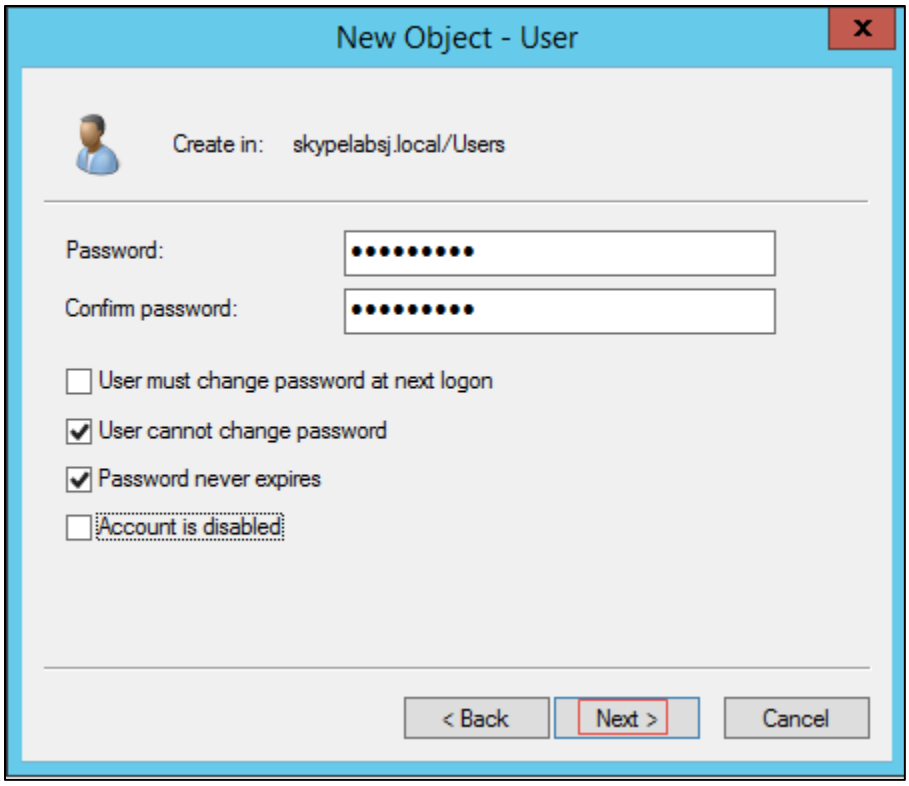


Skype for Business – New User configuration (continued)

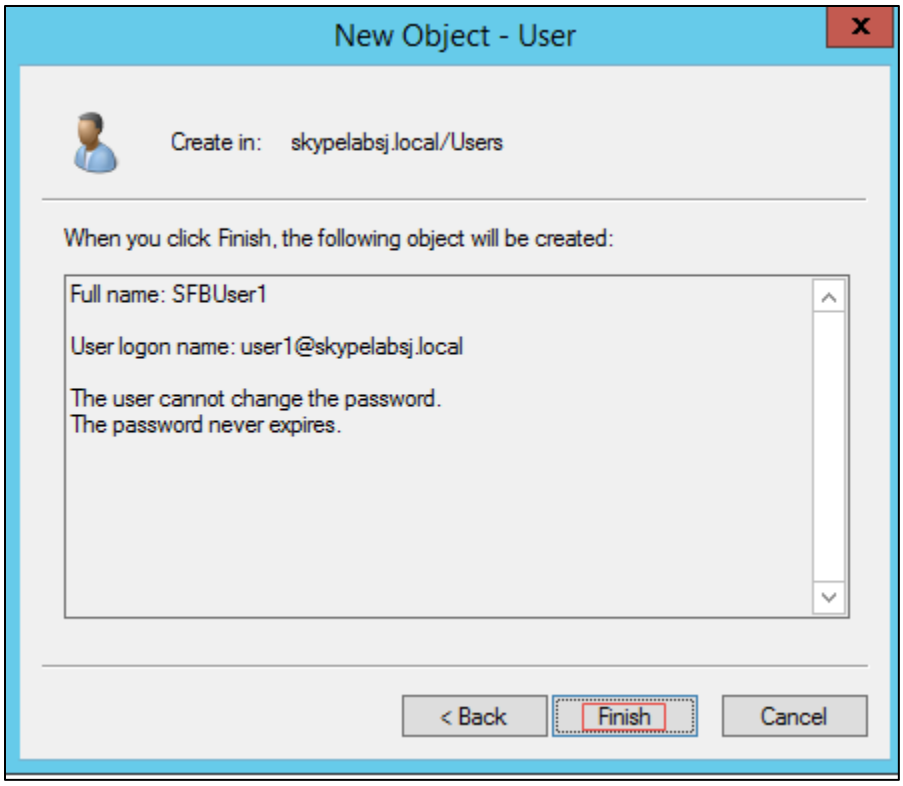
Follow the screenshots below to add a new user:



Skype for Business – New User configuration (continued)



Skype for Business – New User configuration (continued)

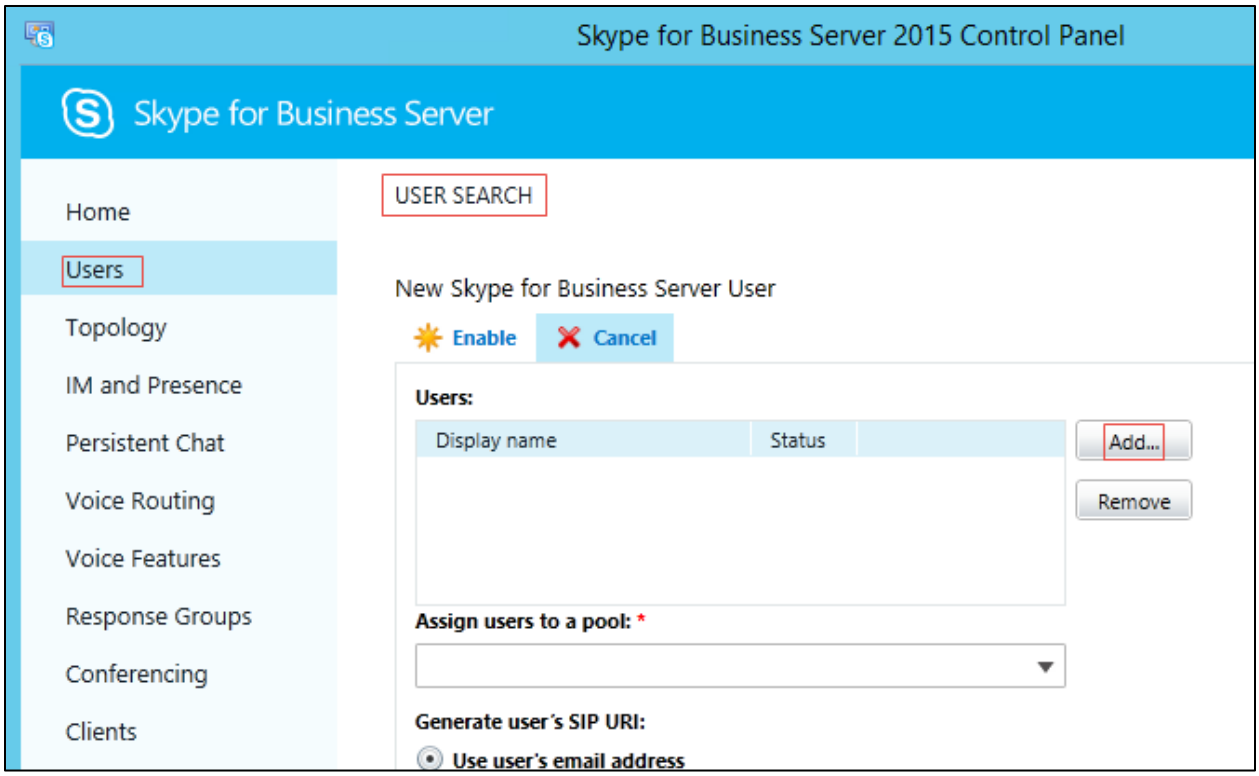


Once the user is created, login to the Skype for Business 2015 Control Panel

Navigation: Users→ Enable users

Click on the Add button and find the new user created earlier.

Skype for Business – New User configuration (continued)



Set Assign users to a pool= FE01.skypelabsj.local from drop down menu

Set Generate user's SIP URI: Specify a SIP URI: sip:SFBUser1@skypelabsj.local .This is used in this test

Set Telephony=Enterprise Voice

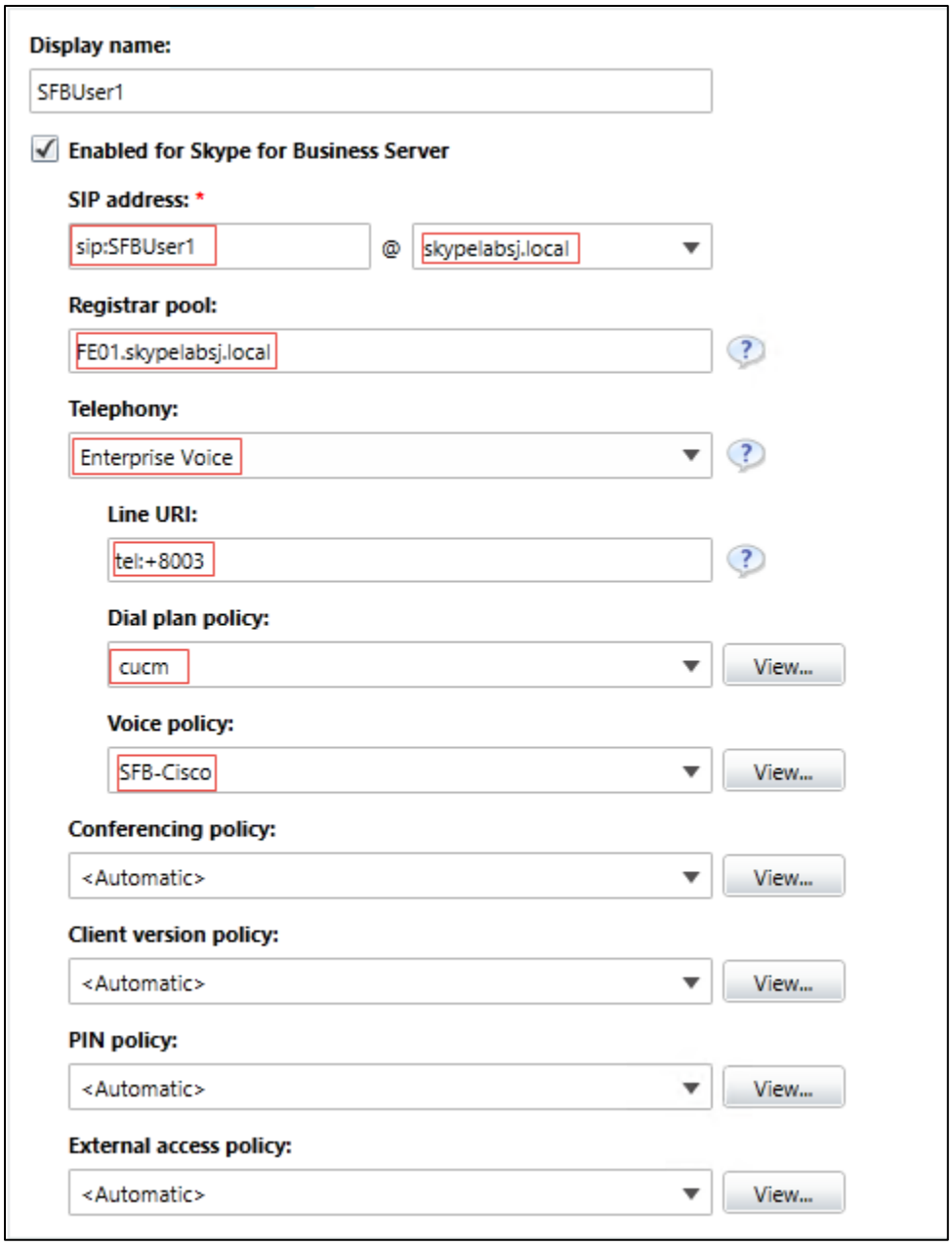
Set Line URI: = tel:+8003 is used for the test. This is the DN for the user.

Set Dial plan policy = cucm (as configured earlier)

Set Voice policy= SFB-Cisco (as configured earlier)

Click Enable.

Skype for Business – New User configuration (continued)

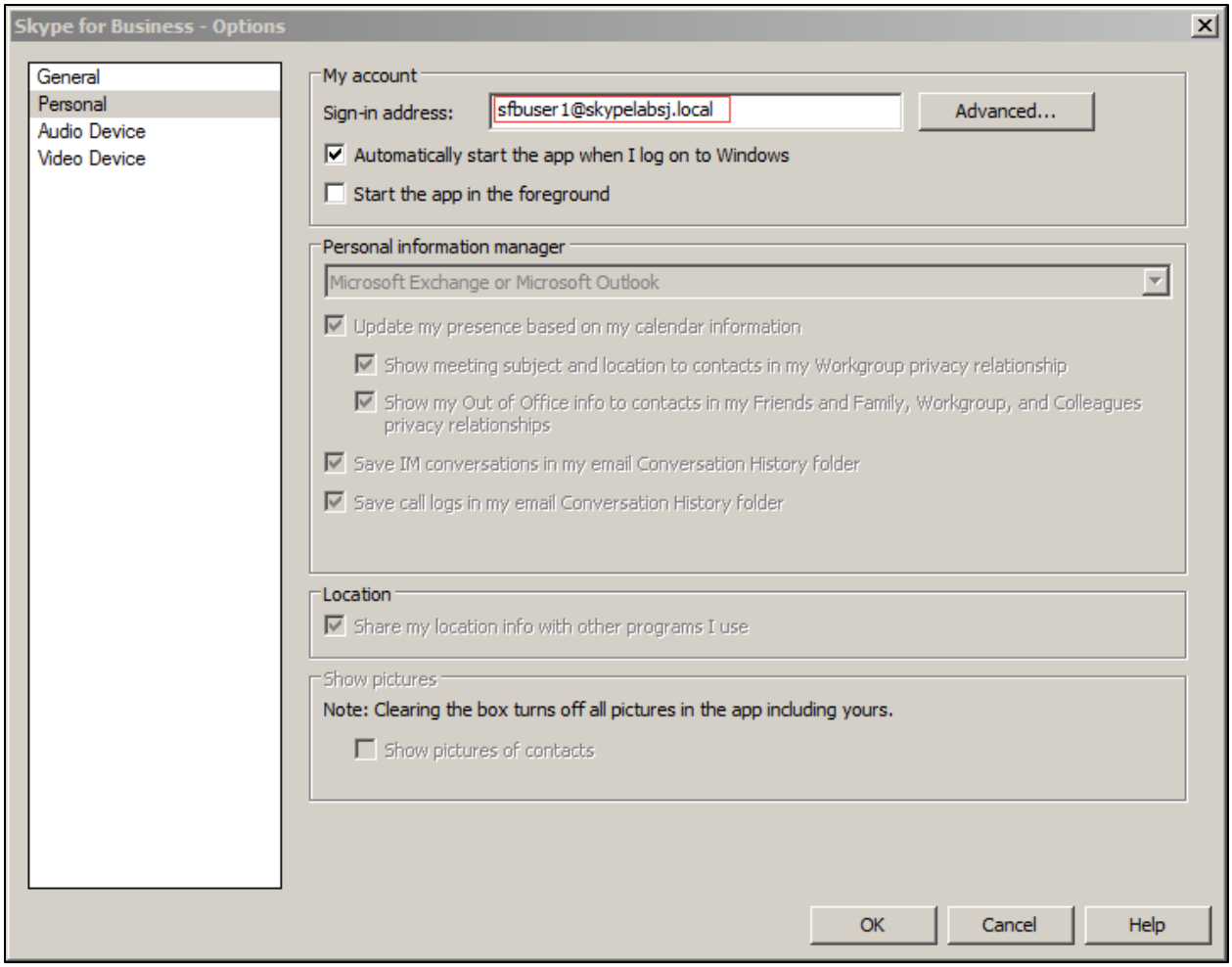


Skype for Business Client Configuration

Download the latest version of the Skype for Business client and launch the same.

Navigation: Settings→Tools→Options→Personal→MyAccount

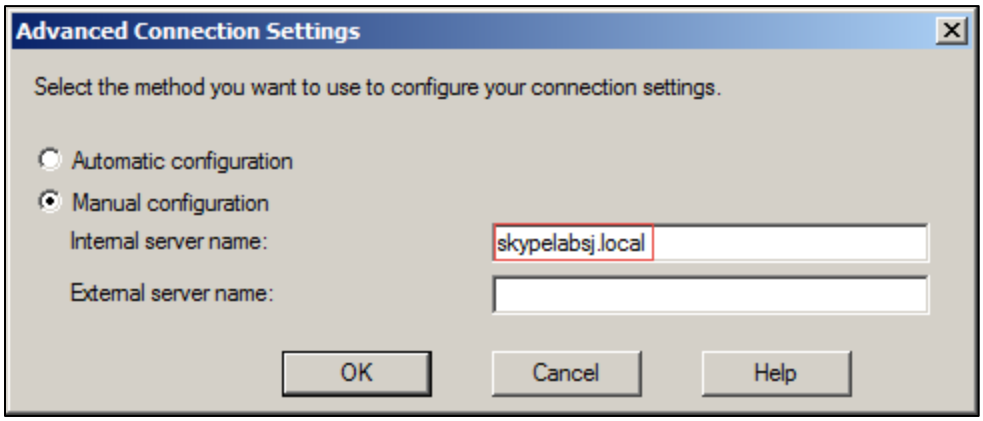
Set Sign-in-address= enter the sip uri of the user configured in username@domain format. sfbuser1@skypelabsj.local is used for example.



Click Advanced. Select Manual Configuration.

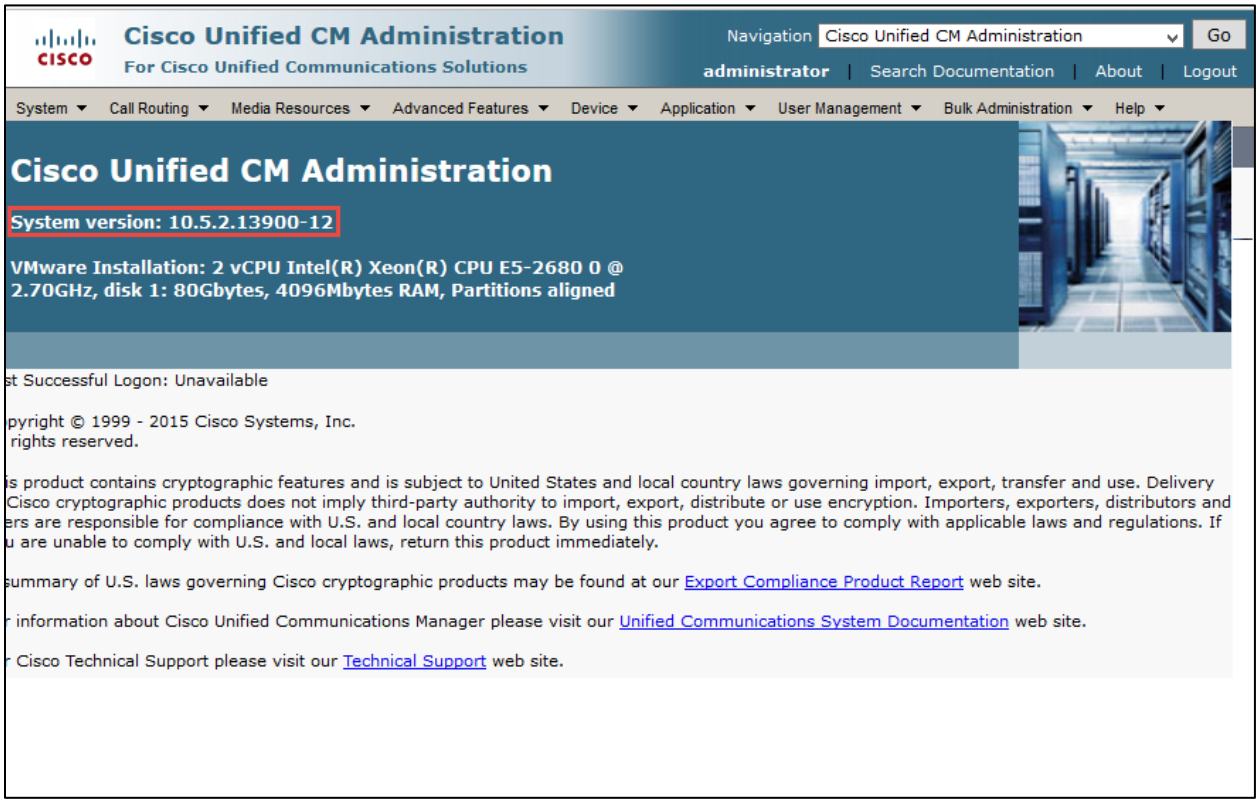
Set Internal Server Name= Enter the FQDN of the domain (skypelabsj.local is used for example)

Skype for Business – Client configuration (continued)



Configuring the Cisco Unified Communications Manager

Cisco Unified Communications Manager Software Version



Cisco Unified Communications Manager SIP Trunk Security Profile for Trunk to Skype for Business

Navigation: System→ Security → SIP trunk security profile

Set Name*= SFB-secure. This is used for the test.

Set Device Security mode = Encrypted

Set Incoming Transport Type = TLS

Set Outgoing Transport Type = TLS

Set X.509 Subject Name = medpool.skypelabsj.local (medpool.skypelabsj.local is the Subject Name of the SIP certificate created in Mediation Server)

Incoming Port = 5061

Check Accept Presence Subscription

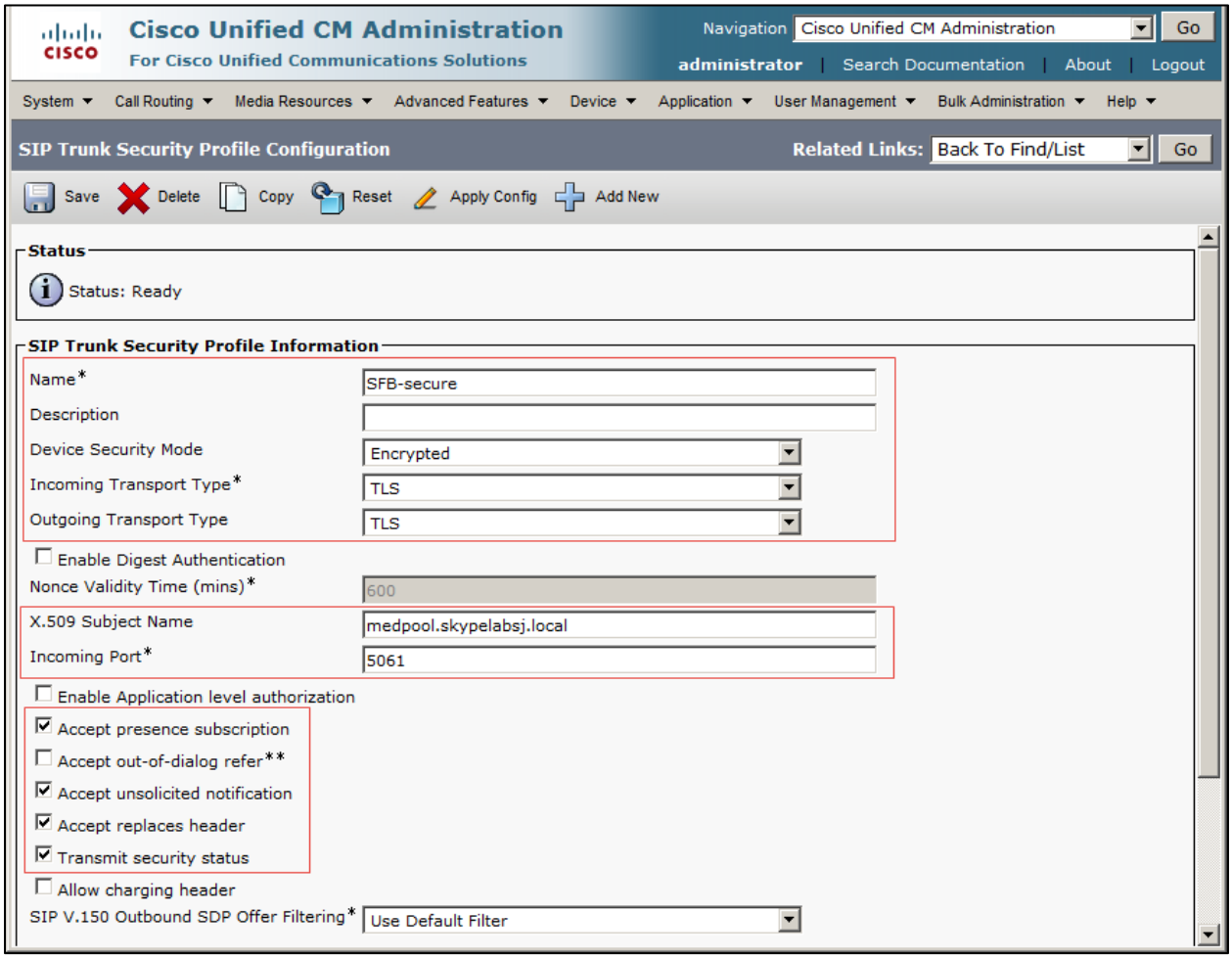
Uncheck Accept out of dialog refer

Check Accept unsolicited notification

Check Accept Replaces header

Check Transmit security status

All other values are default.



Cisco Unified Communications Manager SIP Trunk Security Profile for Trunk to Unity Connection

Navigation: System→ Security → SIP trunk security profile

Set Name*= TLS_CUC. This is used for the test.

Set Device Security mode = Encrypted

Set Incoming Transport Type = TLS

Set Outgoing Transport Type = TLS

Set X.509 Subject Name = TLSConnection (TLSConnection is the Subject Name of the SIP certificate created in Cisco Unity Connection)

Incoming Port = 5061

Uncheck Accept Presence Subscription

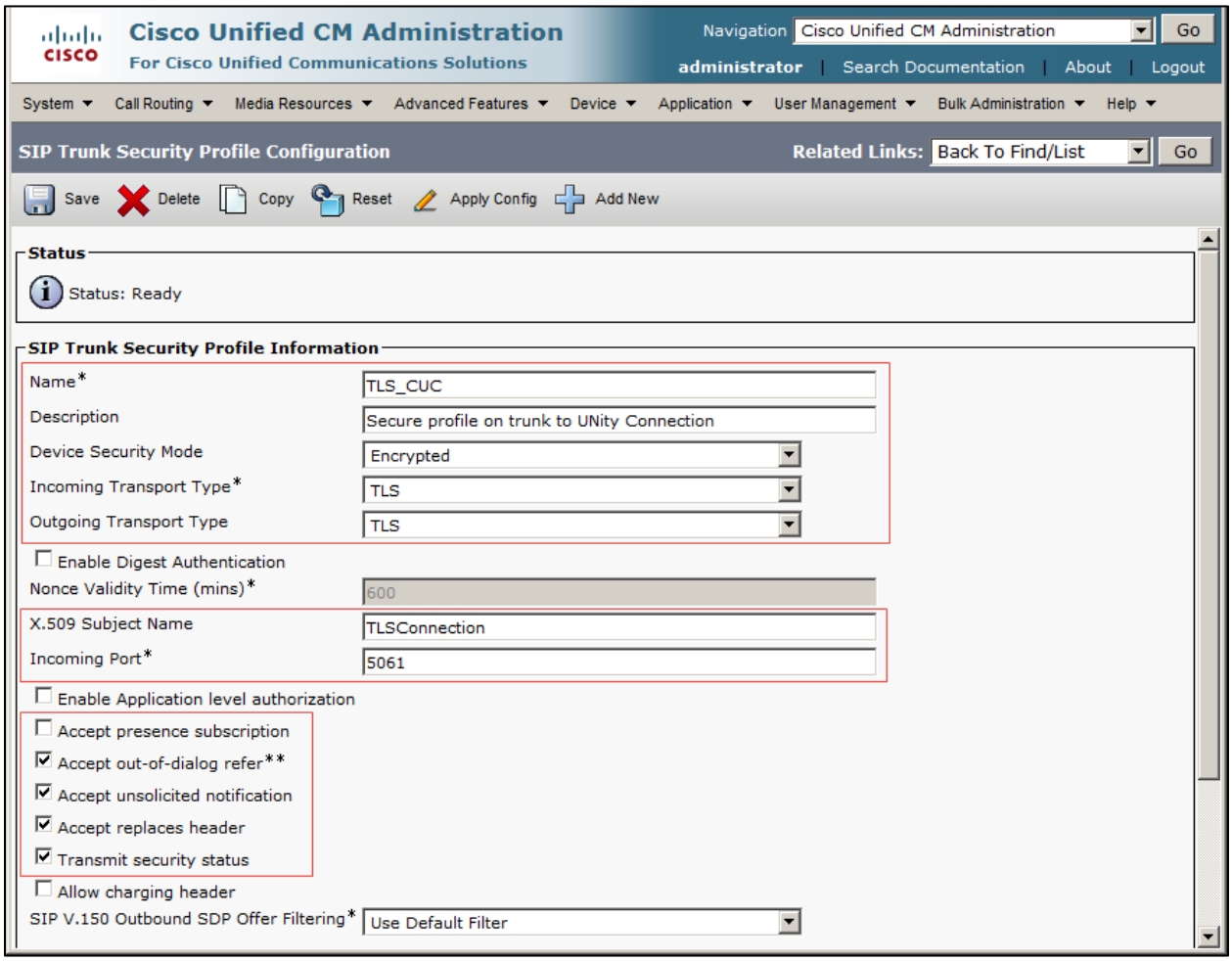
Check Accept out-of-dialog refer**

Check Accept unsolicited notification

Check Accept Replaces header

Check Transmit security status

All other values are default.



Cisco Unified Communications Manager SIP Profile

Navigation: Device → Device Settings → SIP Profile

Set Name*= SFB - Standard SIP Profile. This is used for this test.

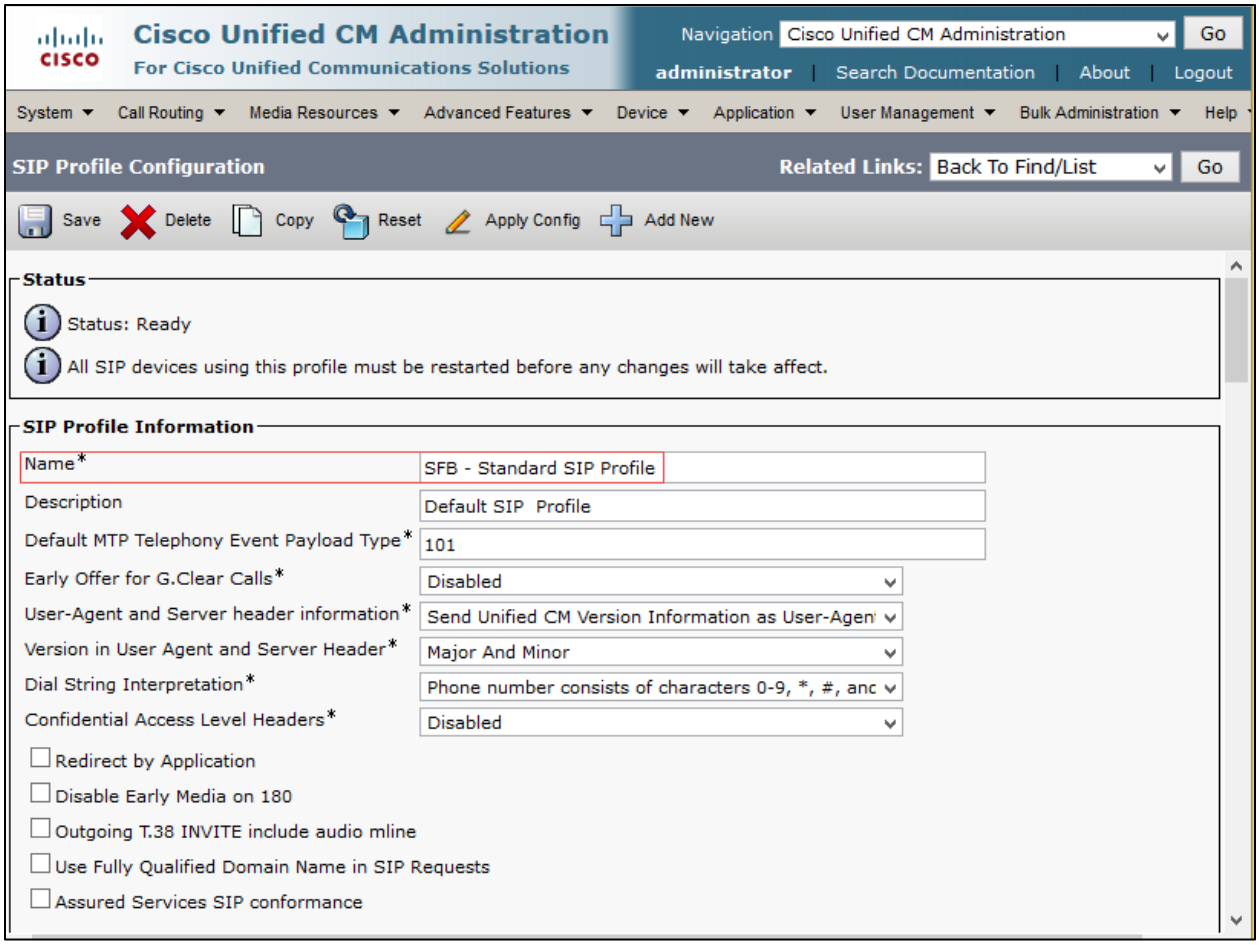
Set Description = this text is used to identify this SIP Profile.

Set SIP Rel1XX Options = Send PRACK if 1xx Contains SDP

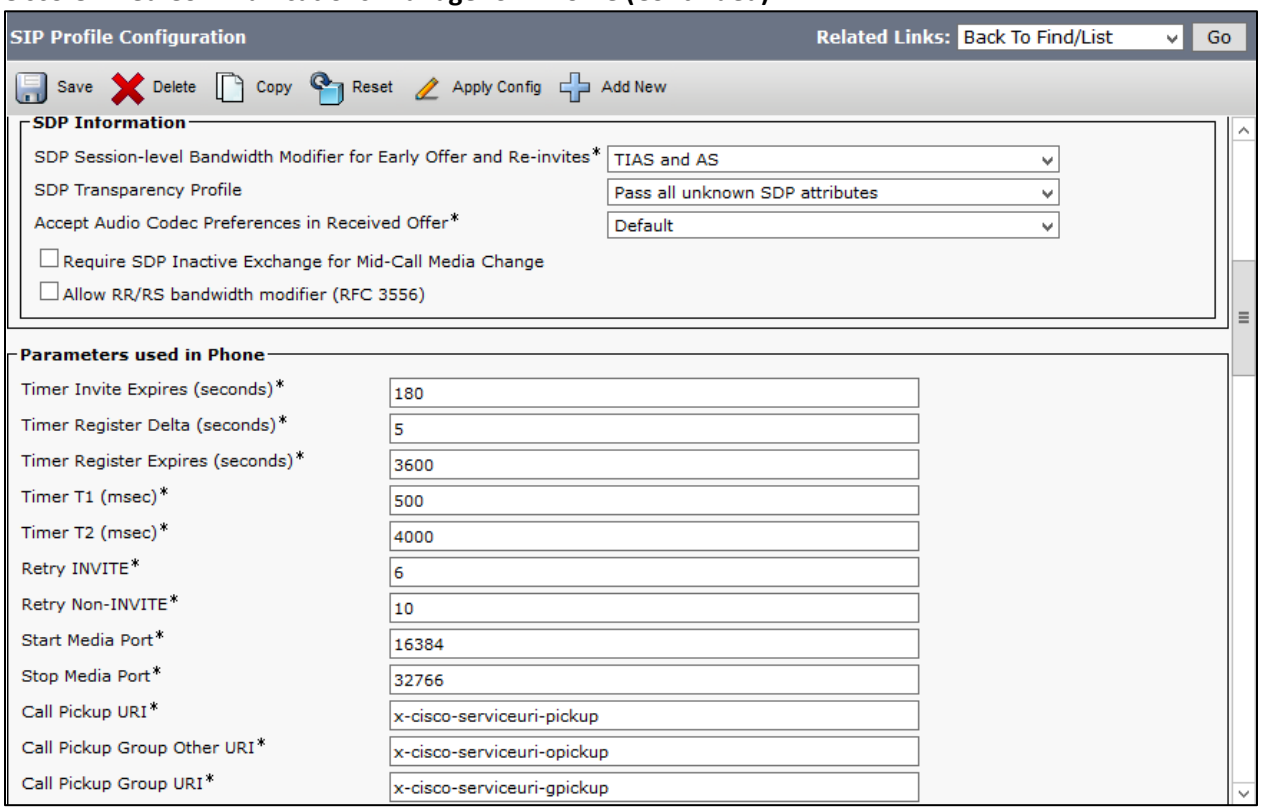
Set Early Offer support for voice and video calls = Best Effort (no MTP inserted)

Check Enable OPTIONS Ping to monitor Destination status for Trunks with Service Type "None (Default)"

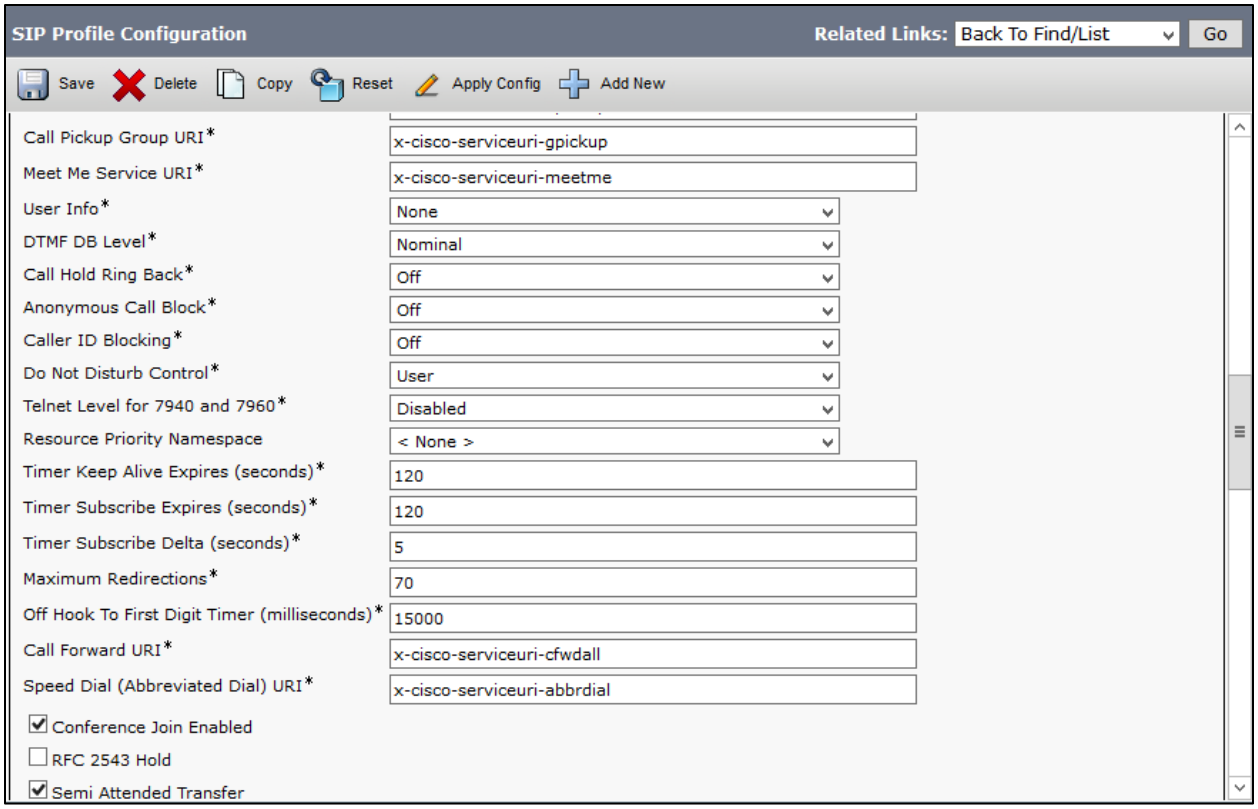
All other values are default.



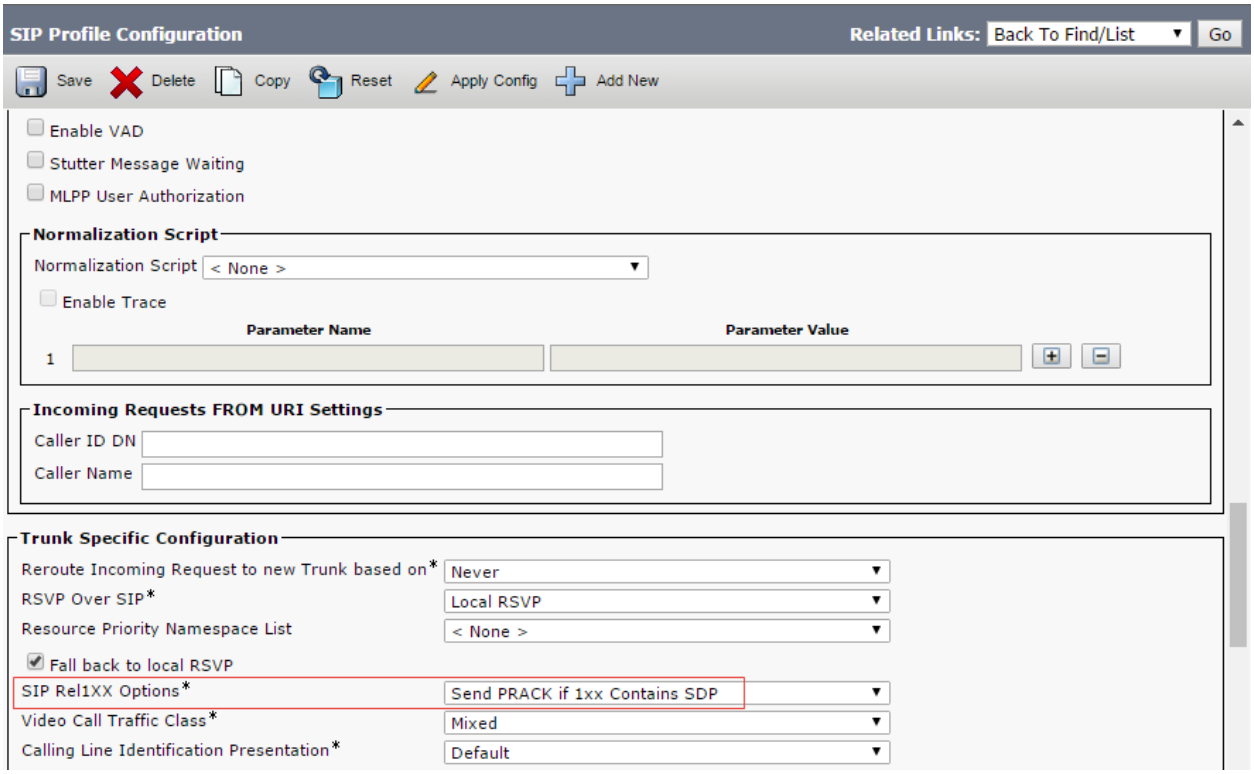
Cisco Unified Communications Manager SIP Profile (Continued)



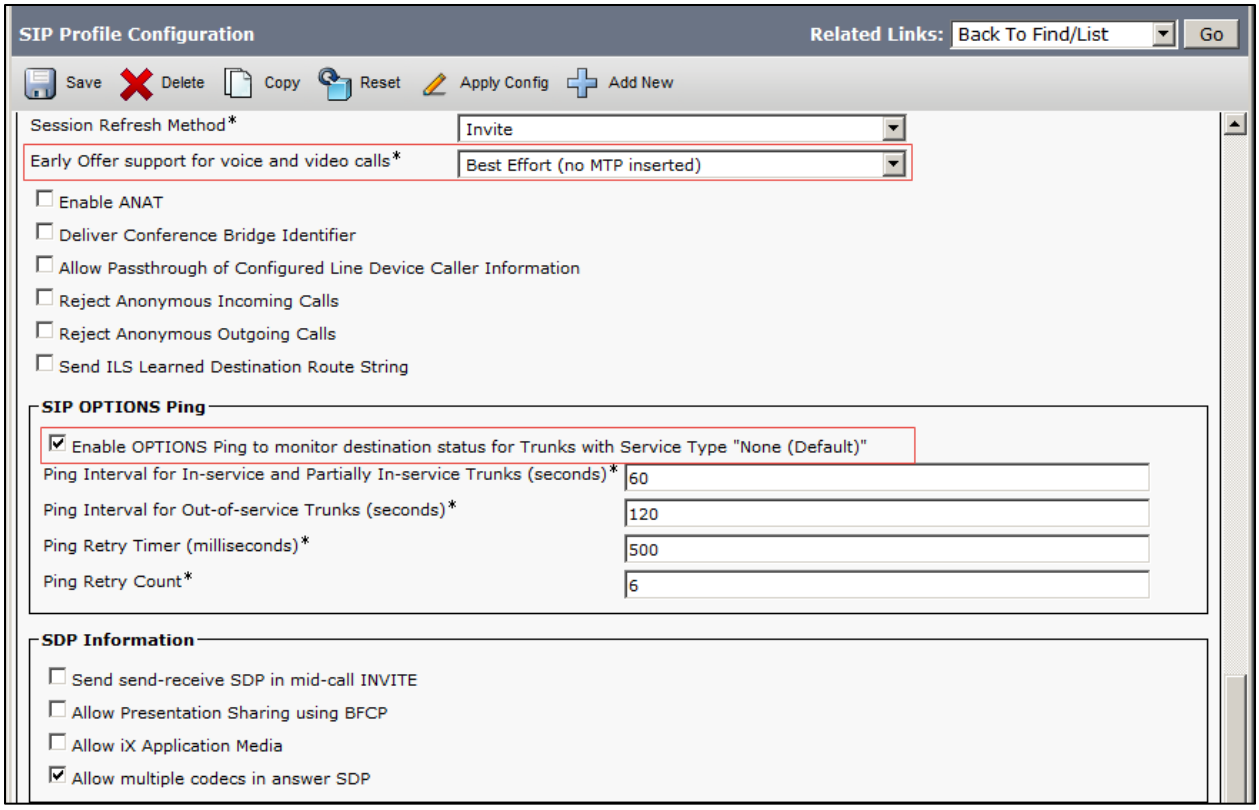
Cisco Unified Communications Manager SIP Profile (Continued)



Cisco Unified Communications Manager SIP Profile (Continued)



Cisco Unified Communications Manager SIP Profile (Continued)



Cisco Unified Communications Manager Media Resource Group

Navigation Path: Media Resources→ Media Resource Group; Add New

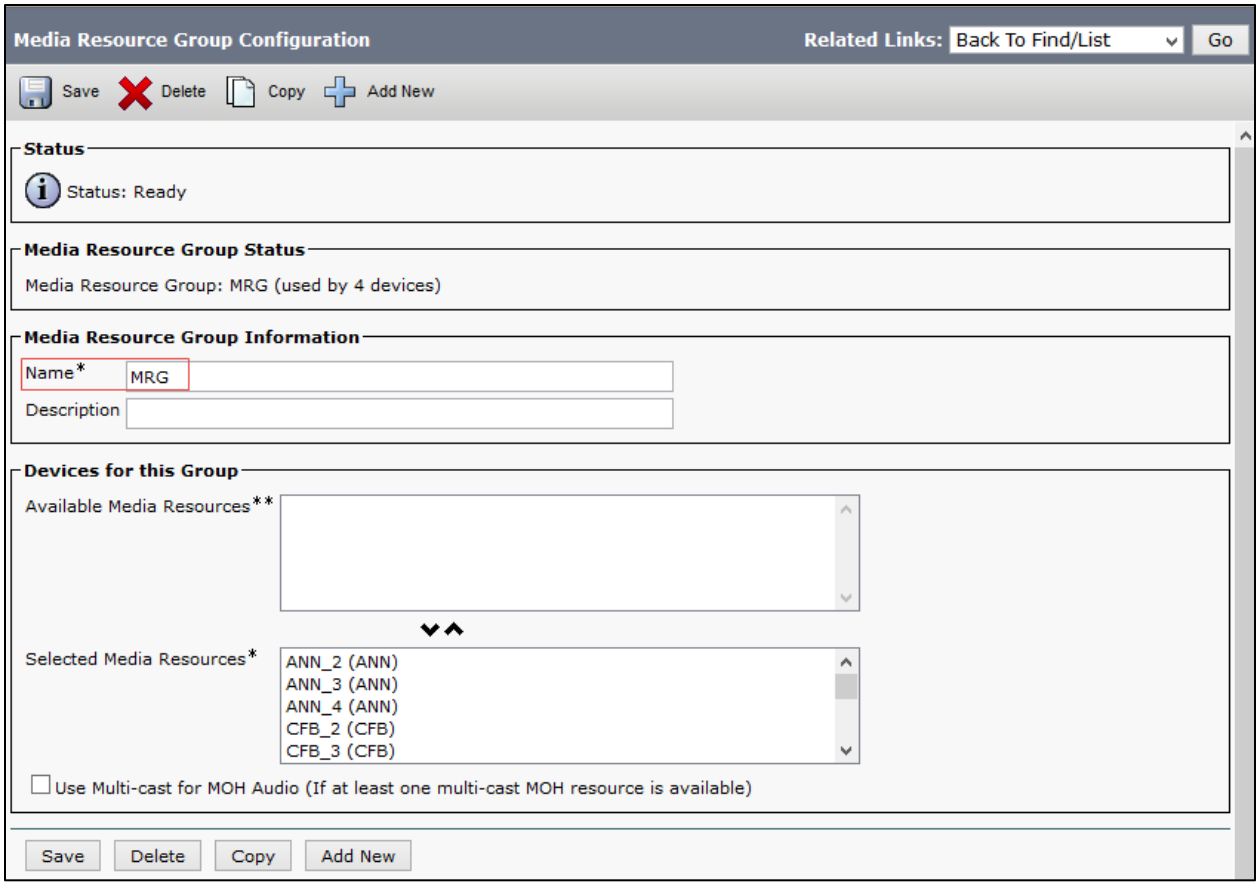
Media Resource Group MRG

Set Name*= MRG, This is used for this test.

Set Description = this text is used to identify this Media Resource Group.

Set all resources in the Selected Media Resources* Box.

All other values are default.



Resource Group for MRG_NoMTP

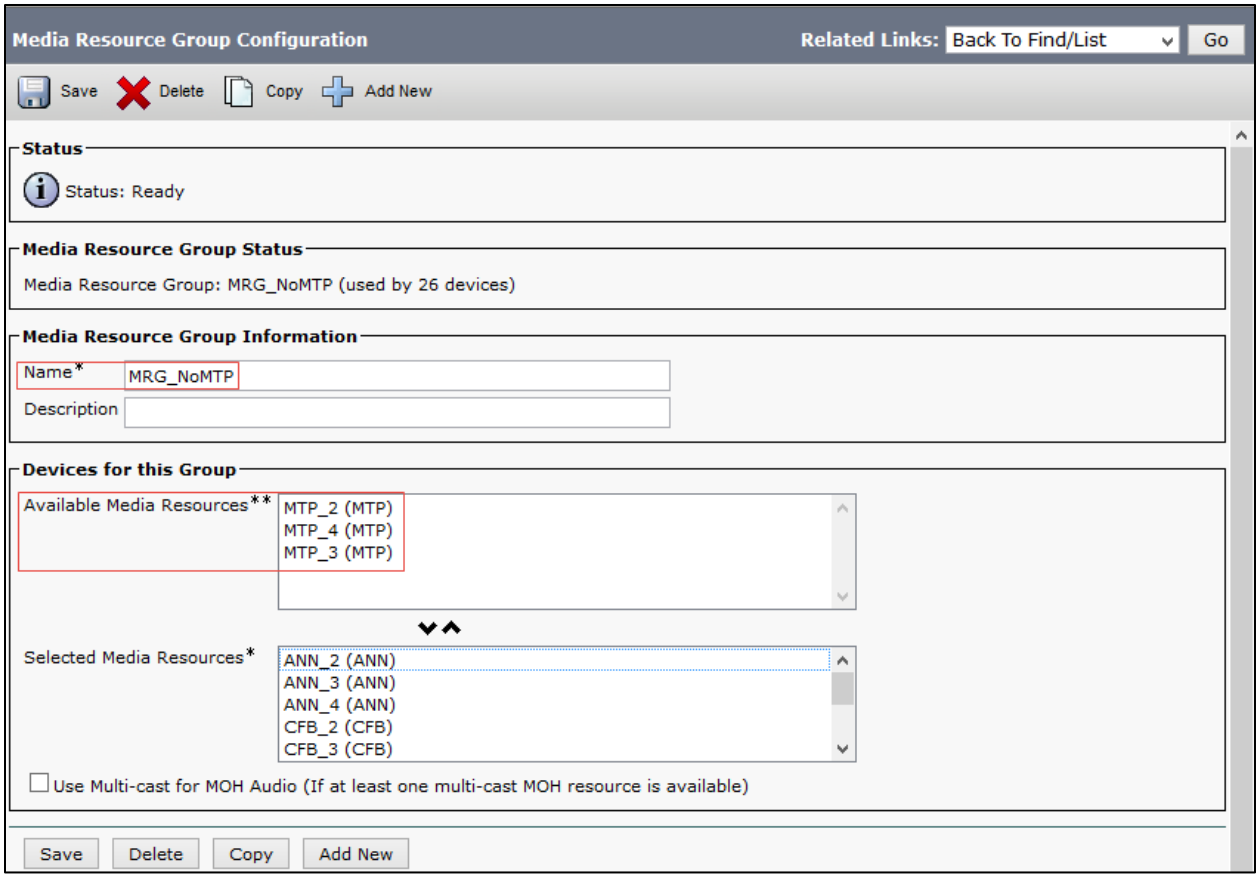
Set Name*= MRG_NoMTP. This is used for the test.

Set Description = this text is used to identify this Media Resource Group.

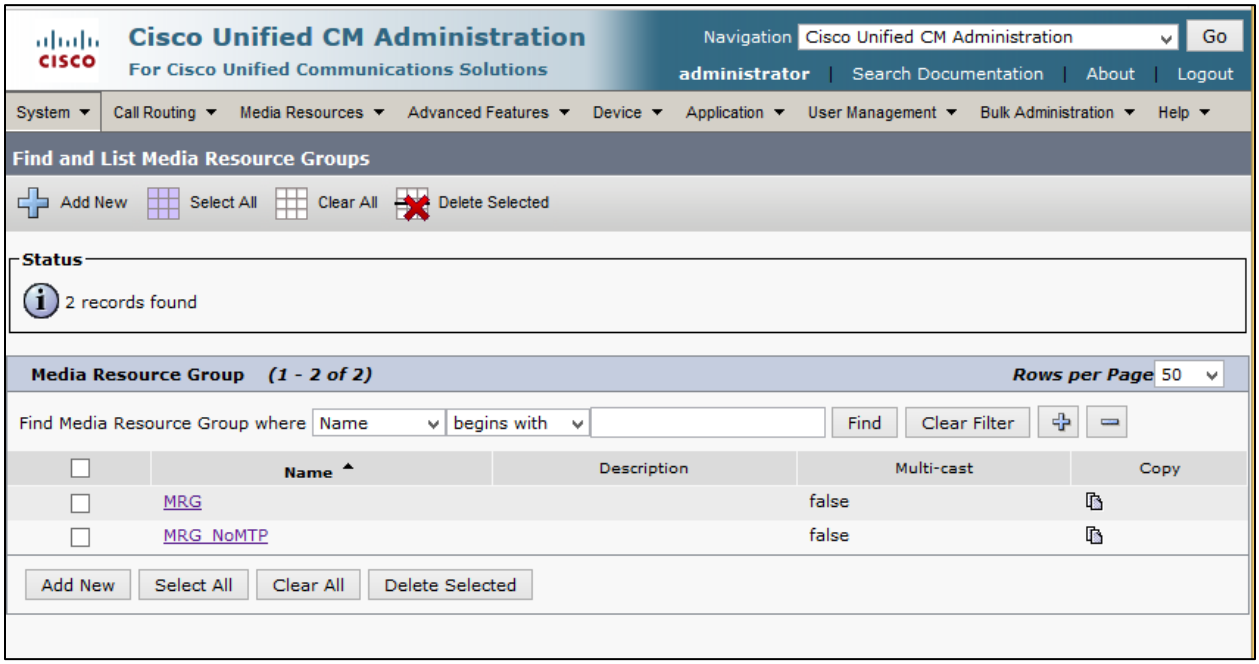
Set Available Media Resources = MTP_2, MTP_3 and MTP_4

Set other resources in the Selected Media Resources*

All other values are default.



Cisco Unified Communications Manager Media Resource Group Configuration



Cisco Unified Communications Manager Media Resource Group List

Navigation Path: Media Resources→ Media Resource Group List

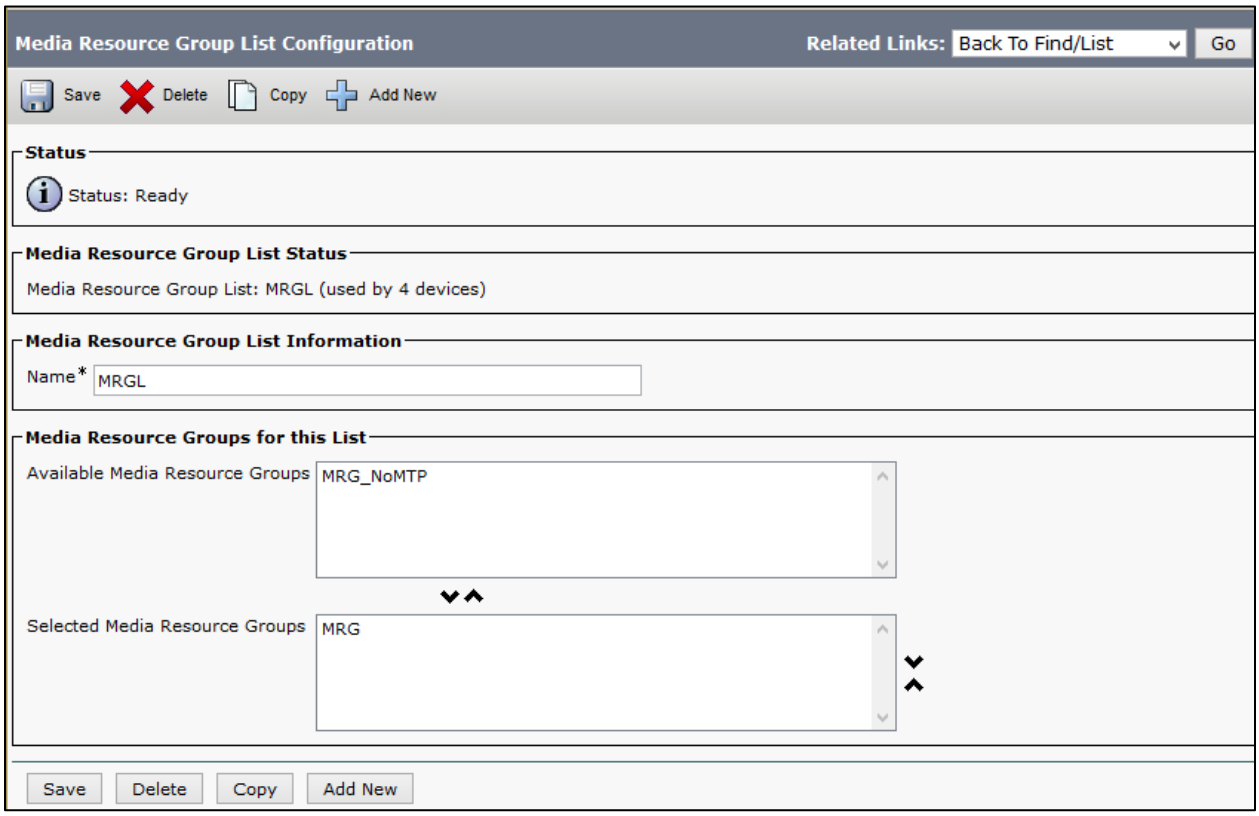
Add New

Set Name*= MRGL. This is used for this test.

Set Description = this text is used to identify this Media Resource Group List.

Set Available Media Resources = MRGL

Set Selected Media Resource Groups= MRG



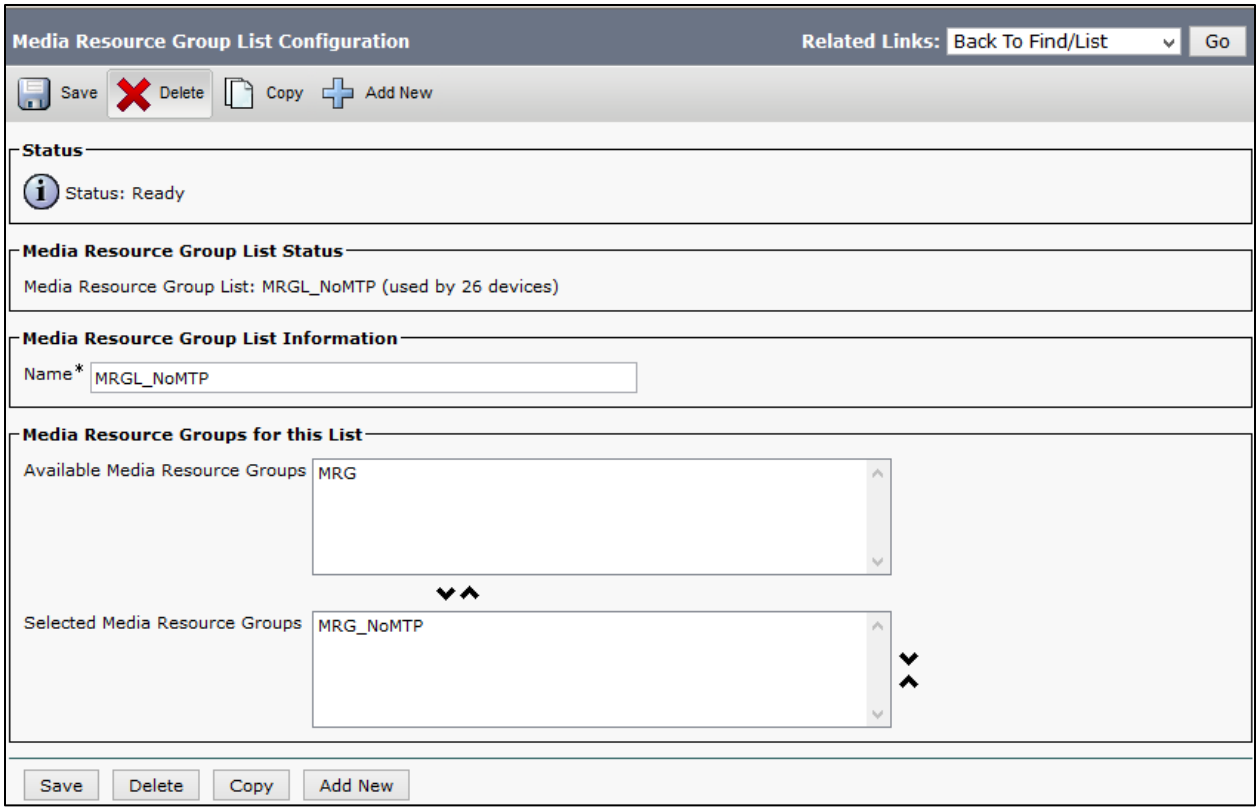
Add new

Set Name*= MRGL_noMTP. This is used for the test

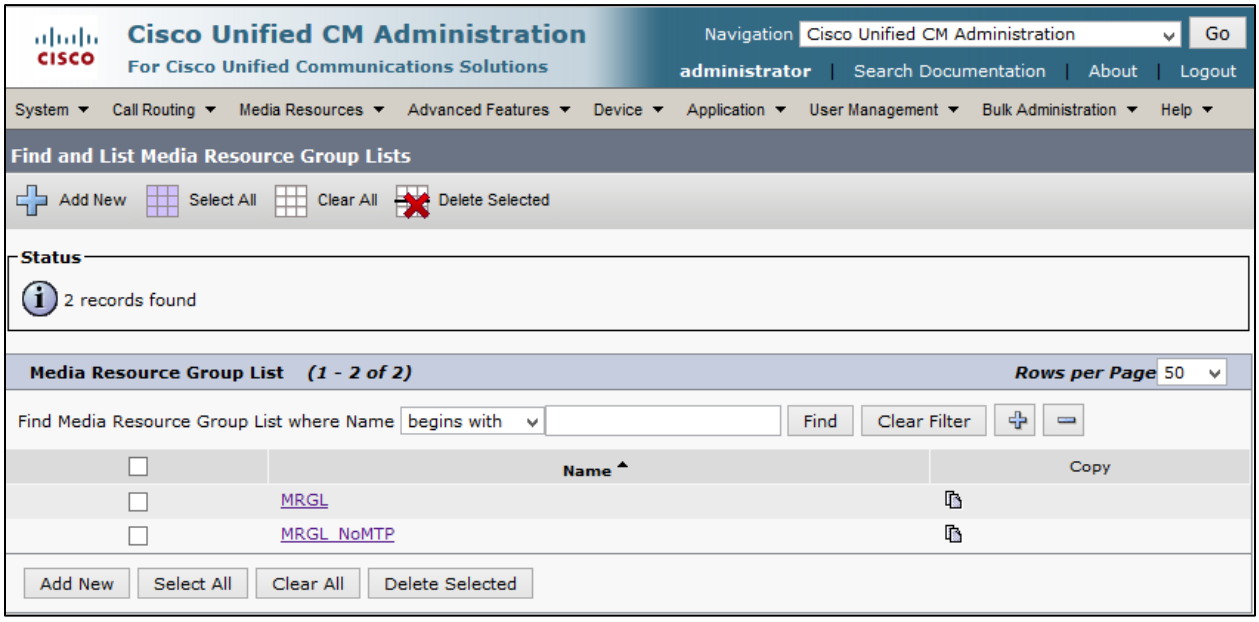
Set Description = this text is used to identify this Media Resource Group List

Set Available Media Resources MRG

Set Selected Media Resource Groups= MRGL_NoMTP



Cisco Unified Communications Manager Media Resource Group List Configuration



Cisco Unified Communications Manager Device Pool Configuration

Device Pool - **G711 Preferred** is created in this test.

Navigation Path: System → Device Pool

Add New.

Set Device Pool Name*= G711 Preferred. This is used in the test.

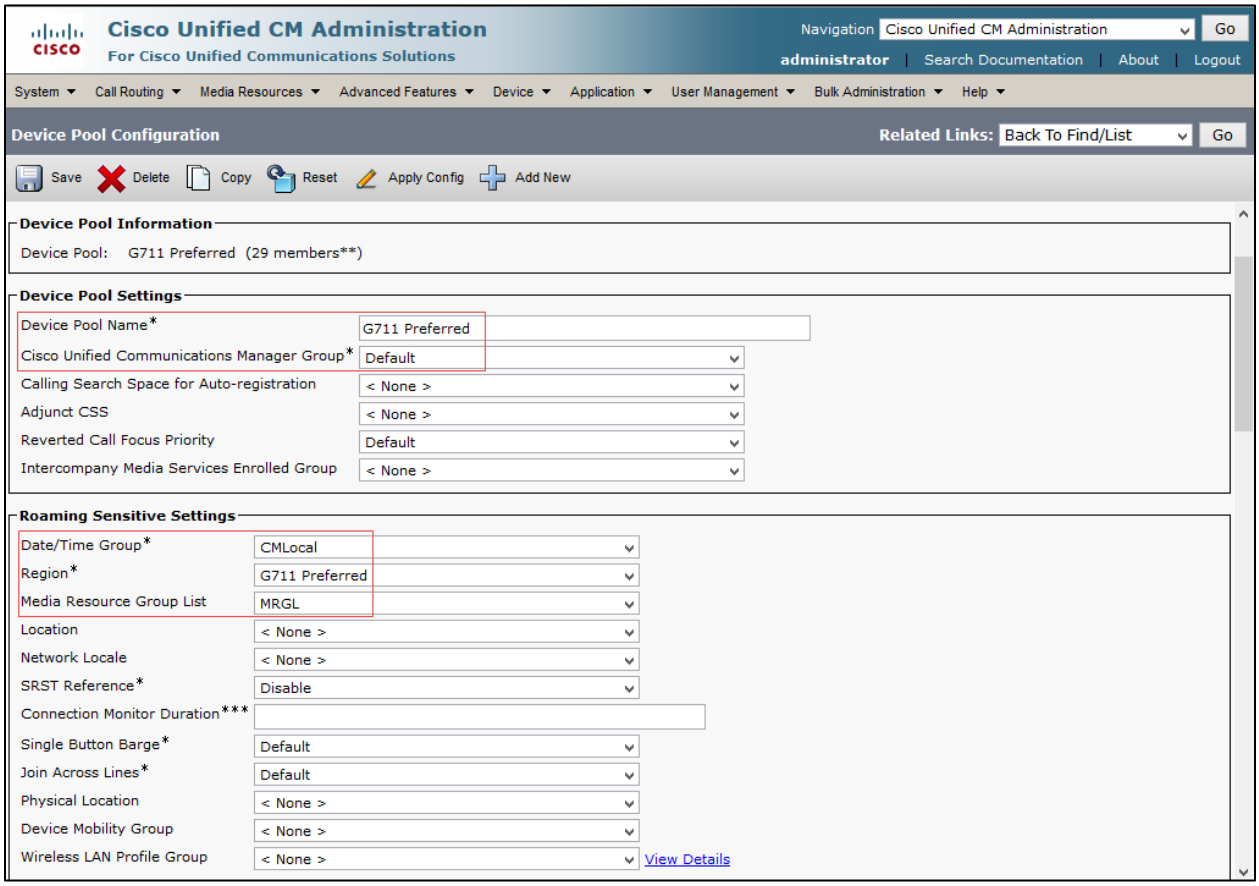
Set Cisco Unified Communications Manager Group*= Default

Set Date/Time Group* = CMLocal

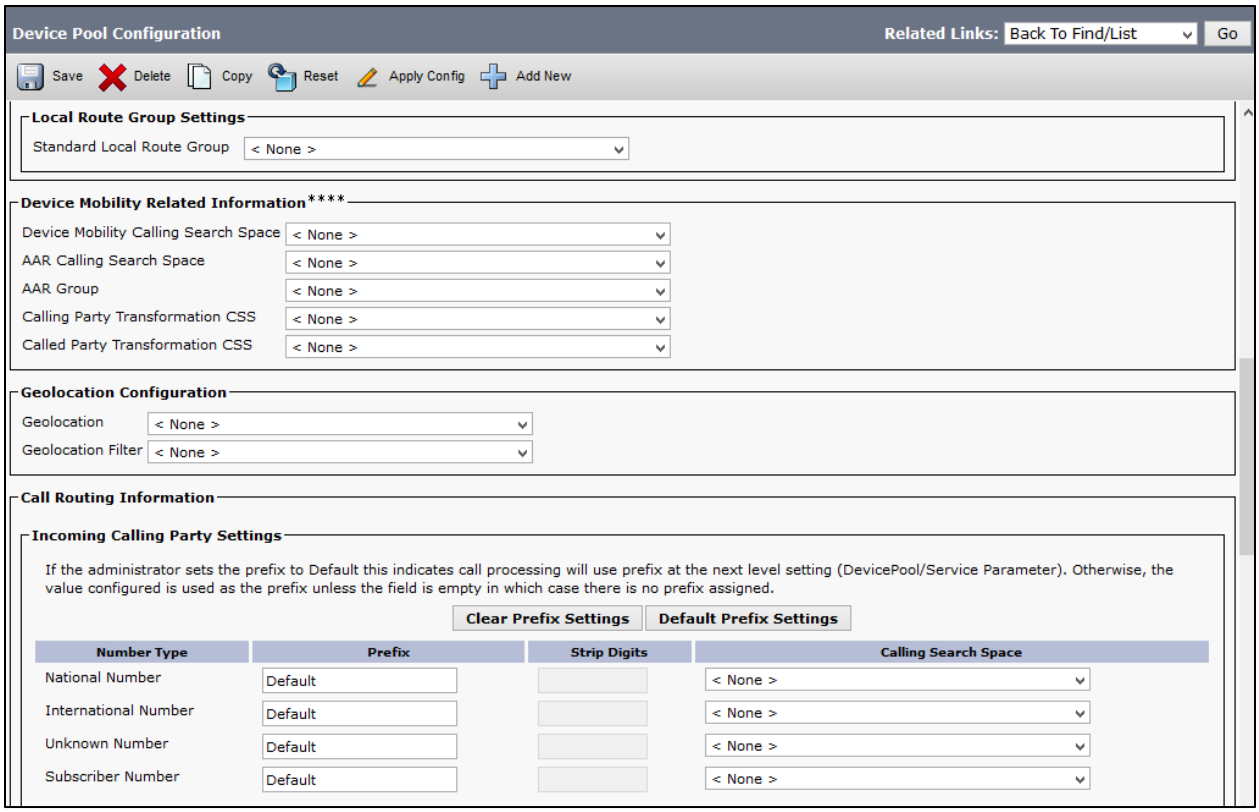
Set Region* = G711 Preferred. This is used in this example

Set Media Resource Group List =MRGL. This is used in this example.

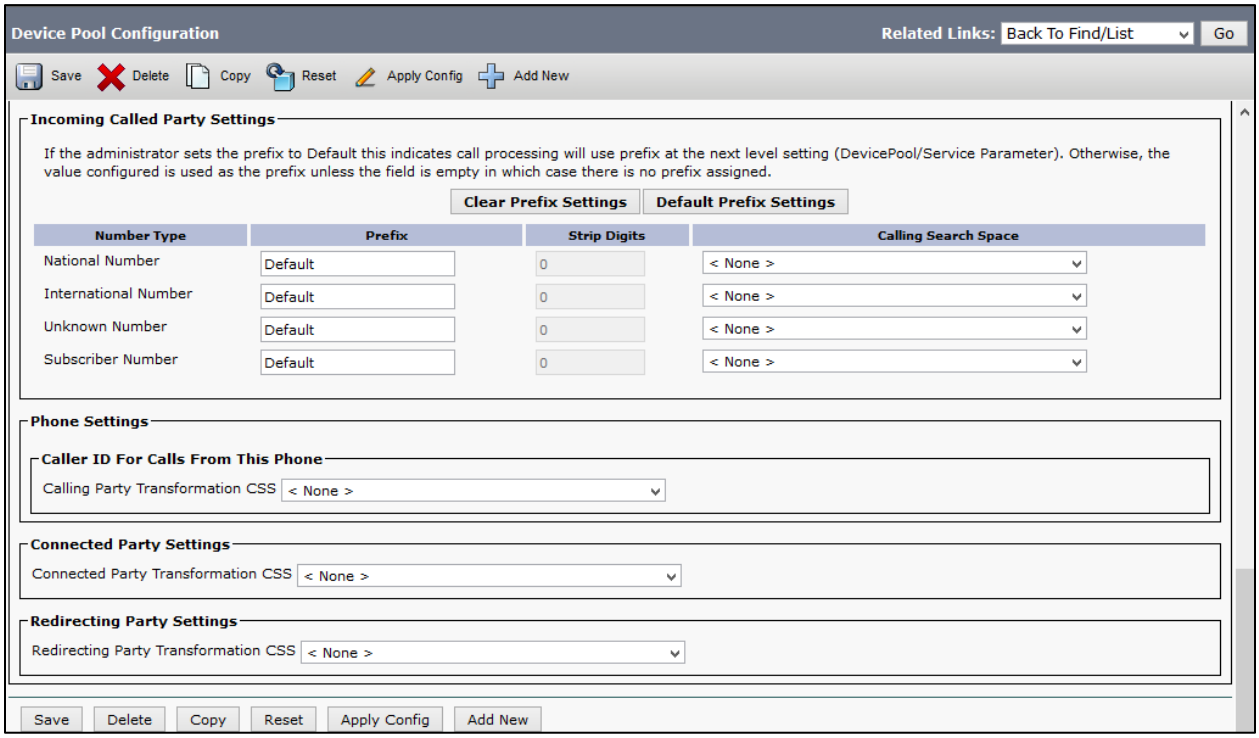
All other values are default.



Cisco Unified Communications Manager Device Pool Configuration (Continued)



Cisco Unified Communications Manager Device Pool Configuration (Continued)



Cisco Unified Communications Manager Region Configuration

Navigation Path: System → Region Information → Region

Add New

G711 Preferred is created in this test.

Set Name*= G711 Preferred. This is used in this example

Set Region= G711 Preferred. This is used in this example

Set Audio Codec Preference List= G711 Preferred

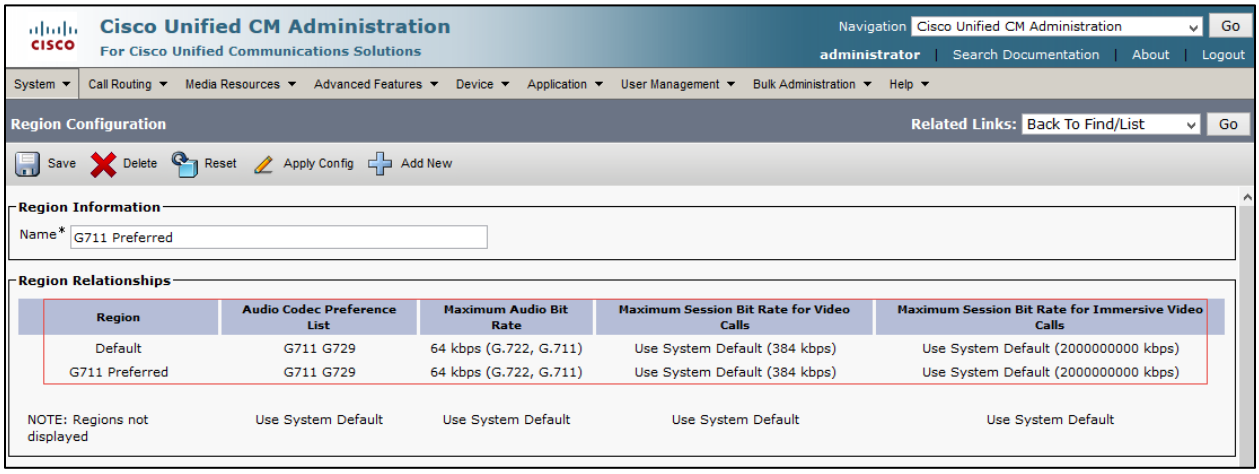
Set Maximum Audio Bit Rate= 64 Kbps (G7.22, G7.11). This is used in this example

Set Region=Default. This is used in this example

Set Audio Codec Preference List= G711 G729. This is used in this example

Set Maximum Audio Bit Rate= 64 Kbps (G722, G7.11). This is used in this example

All other values are default



Cisco Unified Communications Manager Normalization Script

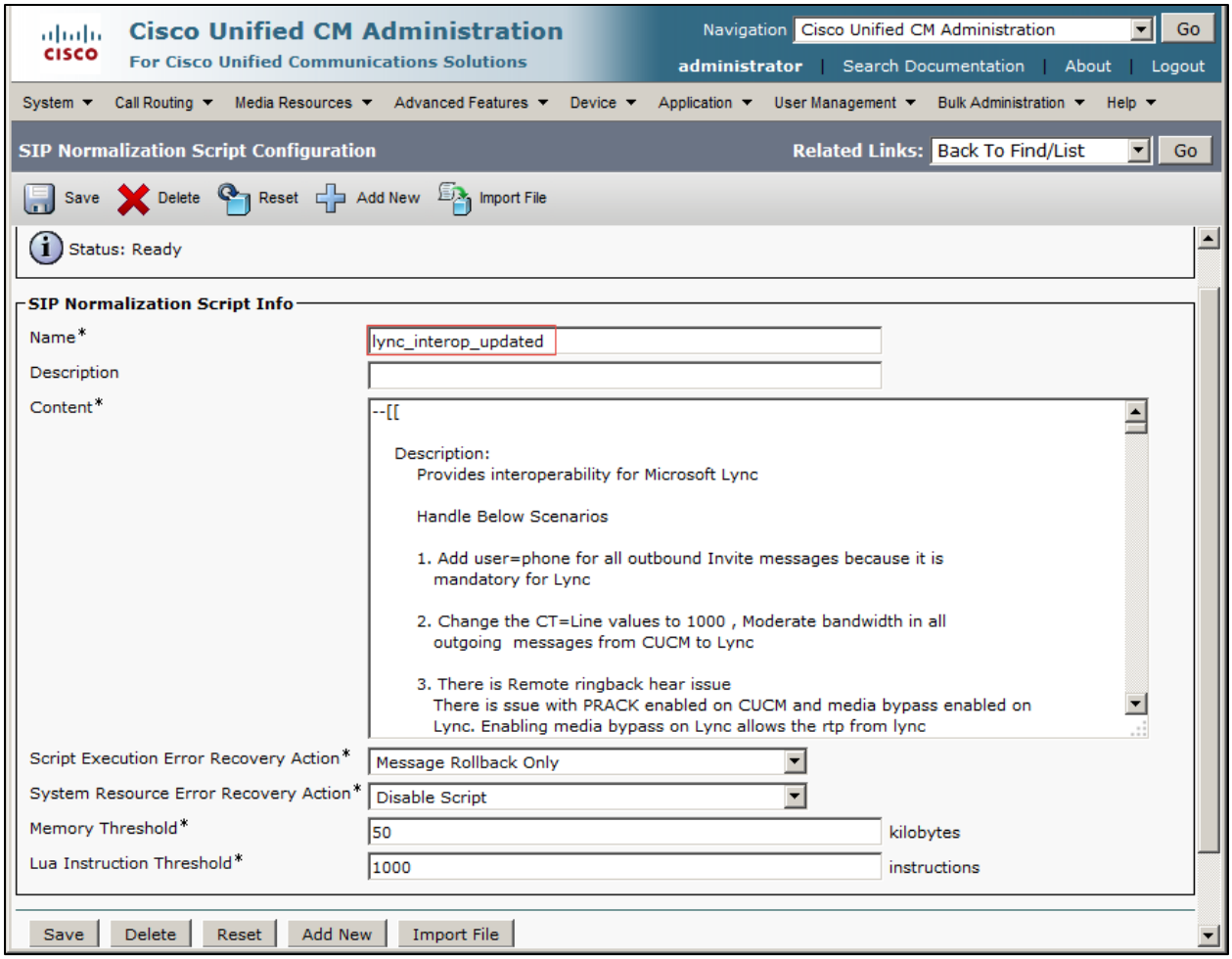
Navigation: Device->Device Settings->SIP Normalization Script

Add New

Set Name = enter text here to identify the normalization script for use on trunk. lync_interop_updated is used in this test.

Set Content = add script content.

Note: “lync_interop” was the originally provided script by Cisco Support for Cisco UCM-Skype for Business TLS integration. However, with the script activated, the call from Skype for Business to Cisco UCM was not established on SRTP still. Cisco UCM sent AVP (that is, chose RTP instead of SRTP) when Skype for Business sent a=tcap:1 RTP/SAVP through INVITE SDP. The script was updated to fix this issue and “lync_interop_updated” is the updated script.



Normalization Script

```
--[[

  Description:
    Provides interoperability for Microsoft Lync

    Handle Below Scenarios

    1. Add user=phone for all outbound Invite messages because it is
       mandatory for Lync

    2. Change the CT=Line values to 1000 , Moderate bandwidth in all
       outgoing  messages from CUCM to Lync

    3. There is Remote ringback hear issue
       There is issue with PRACK enabled on CUCM and media bypass enabled on
       Lync. Enabling media bypass on Lync allows the rtp from lync
       endpoint to flow through CUCM directly instead of flowing through
       mediation server. The problem with PRACK enabled is that Lync end
```

point is now not able to answer the incoming call.Looking into the traces, it appears that even though Lync sent updated connection information in 183 w/sdp, the call manager is still sending rtp to the mediation server which seems to be incorrect" So In this scenario CUCM expects 180 Ringing not 183 Session progress.
So added the Script to convert 183 Session Progress to 180 Ringing.

4. There is incoming Invite from Lync and in From Header there is "user=phone" which cause CUCM to send malformed data in to different layers which cause call failure.So this is work around for that scenario.

5. Script modify the AS header which from outgoing messages because call forward fails due to bandwith negotiation value is A=64 is not supported

6. Script convert the History info to diversion Header since call forward to unity is not supported.

7. Transfer Scenario: Referred-By in Incoming Invite is converted to Diversion Header.

```
   Script Parameters:

   Release: 9.1(2) , 10.0.(1)

   Copyright (c) 2009-2011 Cisco Systems, Inc. All rights reserved.
   All rights reserved.
--]]

M = {}

M.allowHeaders = {"History-Info"}

trace.enable()

local function getDisplayName (i_header)
   local position_of_uri=string.find(i_header, "<")
         if position_of_uri <= 2
         then
                  display_name=nil
         else
                  -- save display name which arrives in quotes
                  local display_name_tmp = string.sub(i_header,1, (position_of_uri - 1))
                  -- now remove the quotes
                  display_name_tmp = string.gsub(display_name_tmp,'"','')
                  -- now remove the space
                  display_name = string.gsub(display_name_tmp,' ','')
```

```
        end
        return display_name
end

local function modify_CT_bandwidth(msg)
   local sdp = msg:getSdp()
   if sdp
   then
      local b_CT_line = sdp:getLine("b=CT","64")
      if not b_CT_line
      then
         local b_CT_line = sdp:getLine("b=CT","0")
         if not b_CT_line
         then
            return
         end
         b_CT_line = b_CT_line:gsub("0", "1000")
         sdp = sdp:modifyLine("b=CT", "0", b_CT_line)
         msg:setSdp(sdp)
         return
      end
      b_CT_line = b_CT_line:gsub("64", "1000")
      sdp = sdp:modifyLine("b=CT", "64", b_CT_line)
      msg:setSdp(sdp)
   end
end

local function remove_AS_bandwidth(msg)
   local sdp = msg:getSdp()
   if sdp
   then
        local b_AS_line = sdp:getLine("b=AS","64")
      if b_AS_line
      then
         sdp = sdp:removeLine("b=AS", "64")
         msg:setSdp(sdp)
      end
   end
end

local function process_outbound_request(msg)

   local method, ruri, ver = msg:getRequestLine()

   if string.find(ruri, "@")
   then
      local uri = ruri .. ";user=phone"
      msg:setRequestUri(uri)
```

```
   end

   modify_CT_bandwidth(msg)
   remove_AS_bandwidth(msg)

end

local function process_outbound_message(msg)
   modify_CT_bandwidth(msg)
   remove_AS_bandwidth(msg)
end


local function process_inbound_progress(msg)

   msg:setResponseCode(180, "Ringing")
   local sdp = msg:getSdp()

         if sdp then
         sdp = sdp:removeMediaDescription("audio")
         msg:setSdp(sdp)
         end

   local req = msg:getHeader("Require")
   local reqHeader = req
   if req
   then
      msg:removeHeader("Require")
   end

   local rseq = msg:getHeader("Rseq")
   local rseqPresnt = rseq
   if rseq
   then
      seqVal = msg:getHeaderValues("Rseq")
      msg:removeHeader("Rseq")
   end

   local sdp = msg:getSdp()
   if sdp
   then
      msg:removeUnreliableSdp()
   end

   if reqHeader
   then
      msg:addHeader("Require", "100rel")
   end
```

```
   if rseqPresnt
   then
     msg:addHeader("RSeq",seqVal[1])
   end
end

-- Future reference for changing cause values in divertion header scenario
-- local HiCauseToDiversion = { }
-- HiCauseToDiversion["302"] = "unconditional"
-- HiCauseToDiversion["486"] = "user-busy"
-- HiCauseToDiversion["408"] = "no-answer"
-- HiCauseToDiversion["480"] = "deflection"
-- HiCauseToDiversion["487"] = "deflection"
-- HiCauseToDiversion["503"] = "unavailable"
-- HiCauseToDiversion["404"] = "unknown"

function convertHIToDiversion(msg)
   local historyInfos = msg:getHeaderValues("History-Info")

   for i, hi in ipairs(historyInfos)
   do
      hi = string.gsub(hi, "%%3B", ";")
      hi = string.gsub(hi, "%%3D", "=")
      hi = string.gsub(hi, "%%22", "\"")
      hi = string.gsub(hi, "%%20", " ")

      -- MS format: <sip:+19728522619@med02.lynclabsj.local;user=phone>;index=1;ms-retarget-
reason=forwarding

      local uri, index, reason = string.match(hi, "<(sip:.*@.*)>;index=(.*)reason=(.*)")

      trace.format("hi: uri '%s', reason '%s'", uri or "nil", reason or "nil")


      if uri
      then
         local diversion = string.format("<%s>", uri)
         if reason
         then
            diversion = string.format("<%s>;reason=\"unconditional\"", uri)
         end
         msg:addHeader("Diversion", diversion)
      end
   end
end

function convertReferredByToDiversion(msg)
```

```
   local refInfo = msg:getHeader("Referred-By")
   if refInfo
   then
      local diversion = string.format("%s;reason=\"unconditional\"", refInfo)
      msg:addHeader("Diversion", diversion)
   end

end

local function replaceHistoryHeader(msg)

   local hist = msg:getHeader("History-Info")

   if hist
   then
      convertHIToDiversion(msg)

      local di  = msg:getHeader("Diversion")

      if di
      then
         msg:removeHeader("History-Info")
      end
   end

end

local function replaceReferredByHeader(msg)

   local refby = msg:getHeader("Referred-By")
   if refby
   then
      convertReferredByToDiversion(msg)
   end

end

local function modifyUserFrom(msg)
-- get a data from "From" header and replace
   local removeUser= ""
   local value = msg:getHeader("From")

   if value
   then
      value = value:gsub(";user=phone", removeUser)
      if value
      then
```

```
        msg:modifyHeader("From", value)
      end
   end
end

local function process_inbound_request(msg)
   modifyUserFrom(msg)
   replaceHistoryHeader(msg)
   replaceReferredByHeader(msg)
   removecryptoline(msg)
   local sdp = msg:getSdp()
    if sdp
    then

       local tcap = sdp:getLine("a=tcap:", "RTP/SAVP")
if
   tcap
      then
      local a_m_line = sdp:getLine("m=audio", "RTP/AVP")
      a_m_line = a_m_line:gsub("AVP", "SAVP")
      sdp = sdp:modifyLine("m=audio", "RTP/AVP", a_m_line)
      end
       sdp=sdp:removeLine("a=crypto:", "|2^31|")
        msg:setSdp(sdp)
    end
end

function process_inbound_any_response(msg)
   msg:addHeader("SUPPORTED","X-cisco-srtp-fallback")
   local sdp = msg:getSdp()

   if sdp
   then
      trace.format("Inbound SDP")
      local tcap = sdp:getLine("a=tcap:", "RTP/SAVP")
      if tcap
      then
         local a_m_line = sdp:getLine("m=audio", "RTP/AVP")
         a_m_line = a_m_line:gsub("AVP", "SAVP")
         sdp = sdp:modifyLine("m=audio", "RTP/AVP", a_m_line)
      end
      trace.format("before removing crypto")
      sdp=sdp:removeLine("a=crypto:", "|2^31|")
      trace.format("after removing crypto")
      msg:setSdp(sdp)
   end
end
```

```
function removecryptoline(msg)
   local sdp = msg:getSdp()
   if sdp
   then
      trace.format("removecryptoline before removing crypto")
      sdp=sdp:removeLine("a=crypto:", "|2^31|")
      trace.format("removecryptoline after removing crypto")
      msg:setSdp(sdp)
   end

end


function process_inbound_any_request(msg)
  msg:addHeader("SUPPORTED","X-cisco-srtp-fallback")
end

M.outbound_INVITE        = process_outbound_request
M.outbound_ACK           = process_outbound_message
M.outbound_200_INVITE    = process_outbound_message
M.outbound_18X_INVITE    = process_outbound_message

M.inbound_183_INVITE     = process_inbound_progress
M.inbound_INVITE         = process_inbound_request
M.inbound_ANY_ANY        = process_inbound_any_response
M.inbound_ANY            = process_inbound_any_request

return M
```

Cisco Unified Communications Manager SIP Trunk to Skype for Business Configuration

Navigation: Device → Trunk

Set Device Name*= SFB-MedPool-CUCM. This is used for the test

Set Description = this text is used to identify this Trunk Group

Set Device Pool* = G711 Preferred. This is used for the test

Set Call Classification*= Use System Default. This is used for the test

Set Media Resource Group List = MRGL. This is used for the test

Uncheck Media Termination Point Required

Check Run On All Active Unified CM Nodes

Check Redirecting Diversion Header Delivery – Inbound

Set Destination Address = medpool.skypelabsj.local. [FQDN of Skype for Business Mediaition Pool] This is used in the test

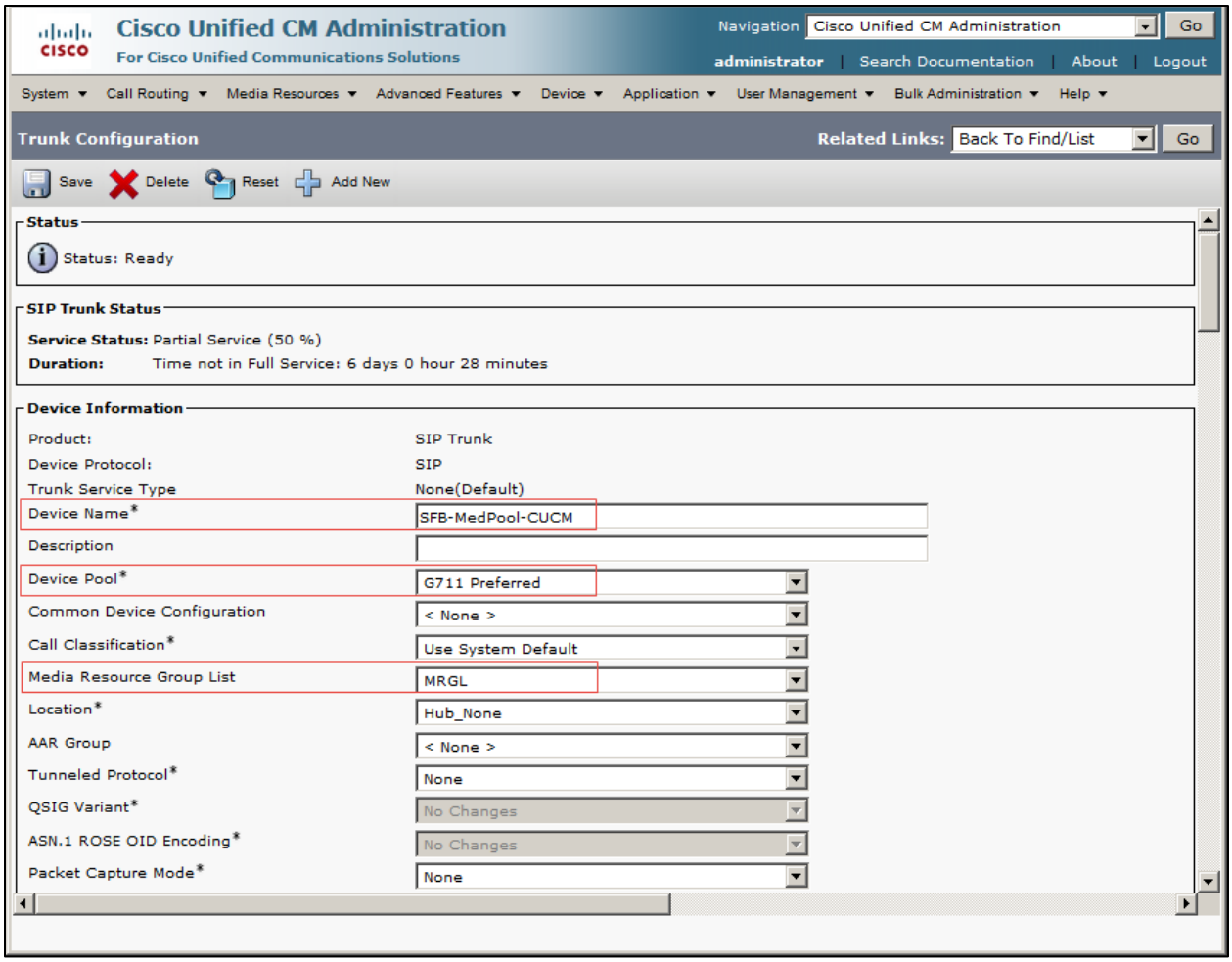
Set SIP Trunk Security Profile*= SFB-secure

Set SIP Profile*= SFB – Standard SIP Profile

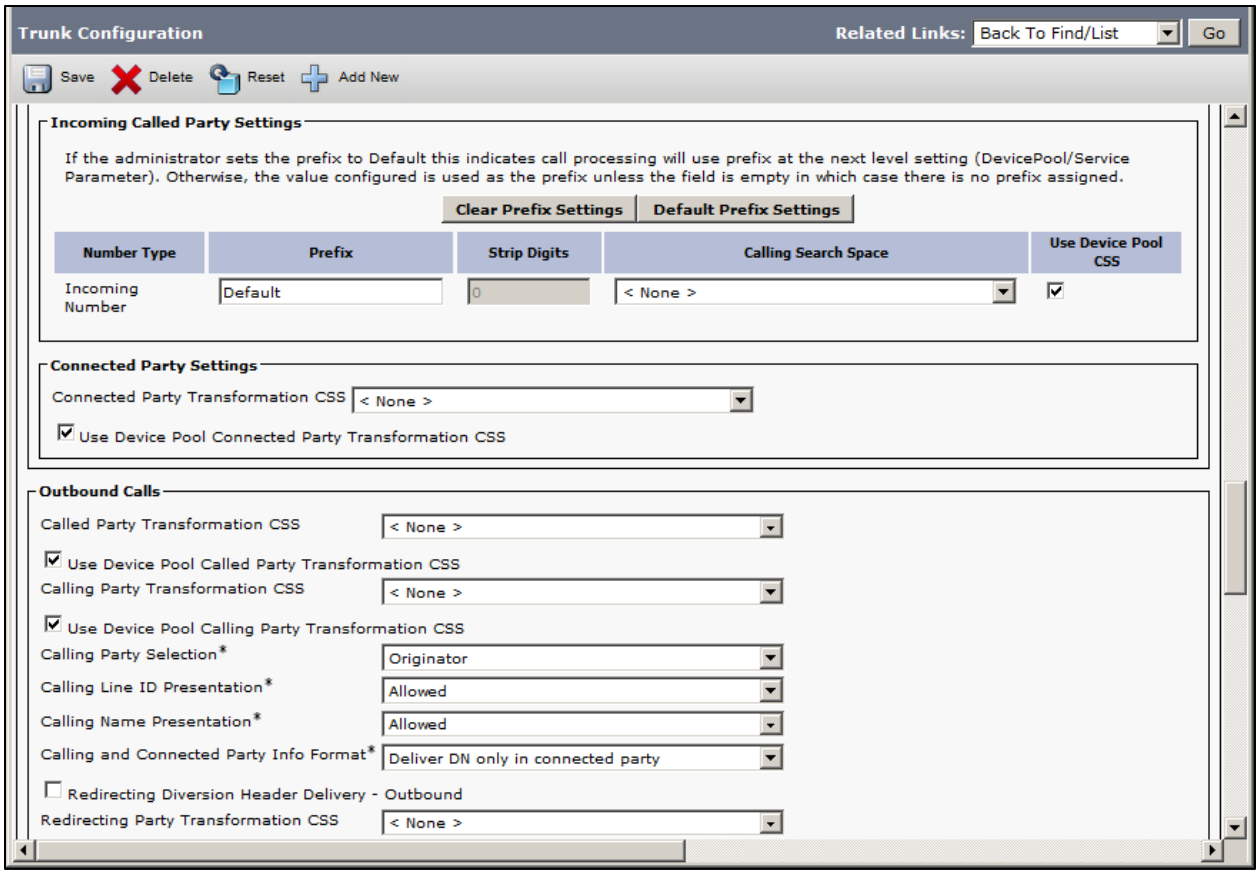
Set DTMF Signaling Method*= RFC 2833

Set Normalization Script = lync_interop_updated

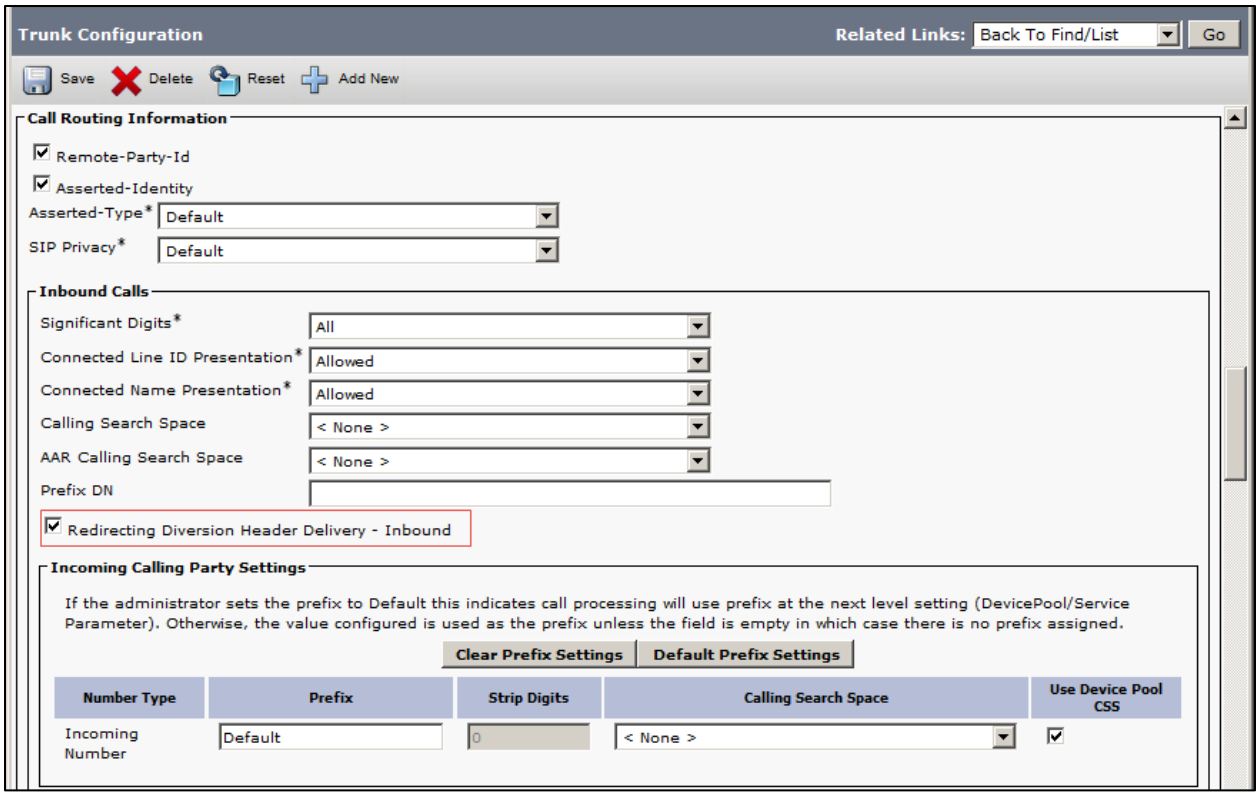
All other values are default.



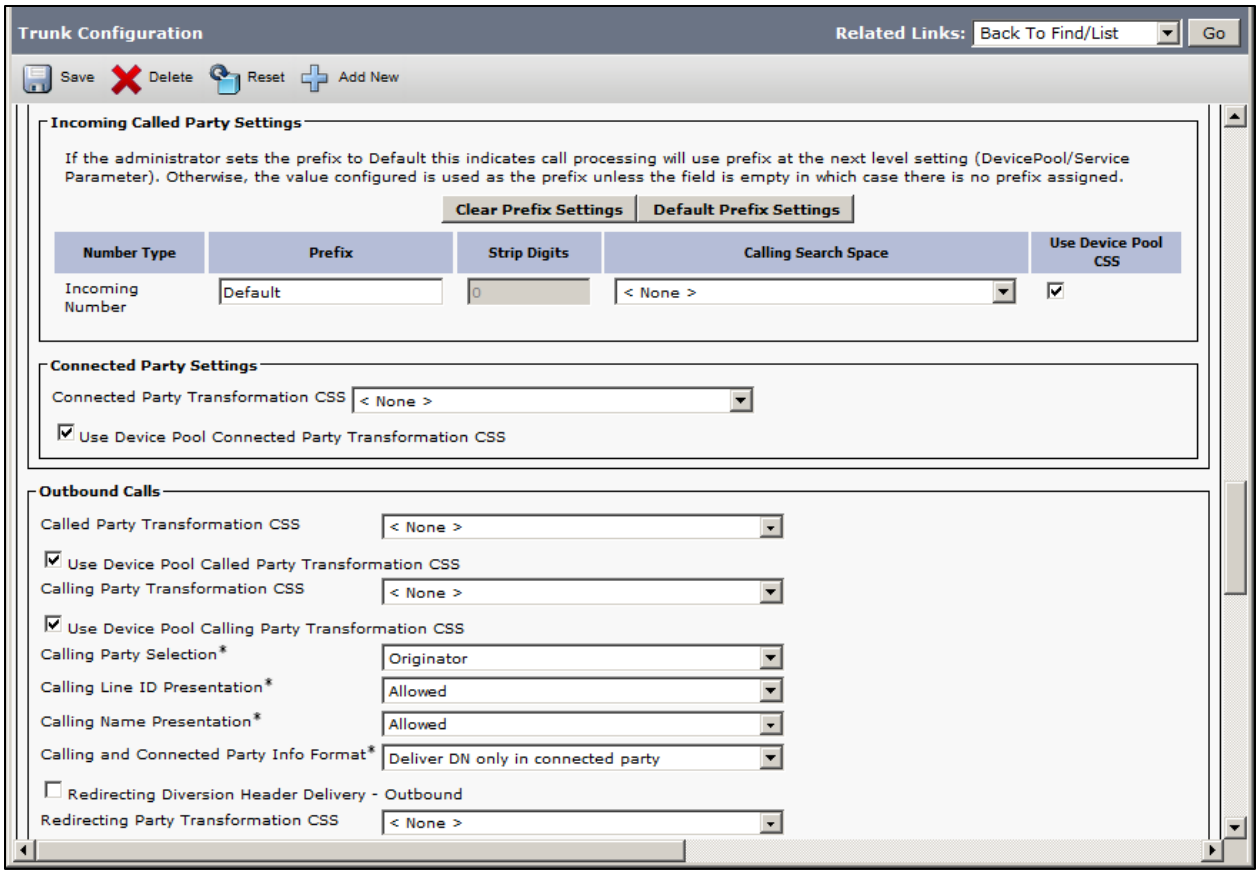
Cisco Unified Communications Manager SIP Trunk to Skype for Business Configuration (Continued)



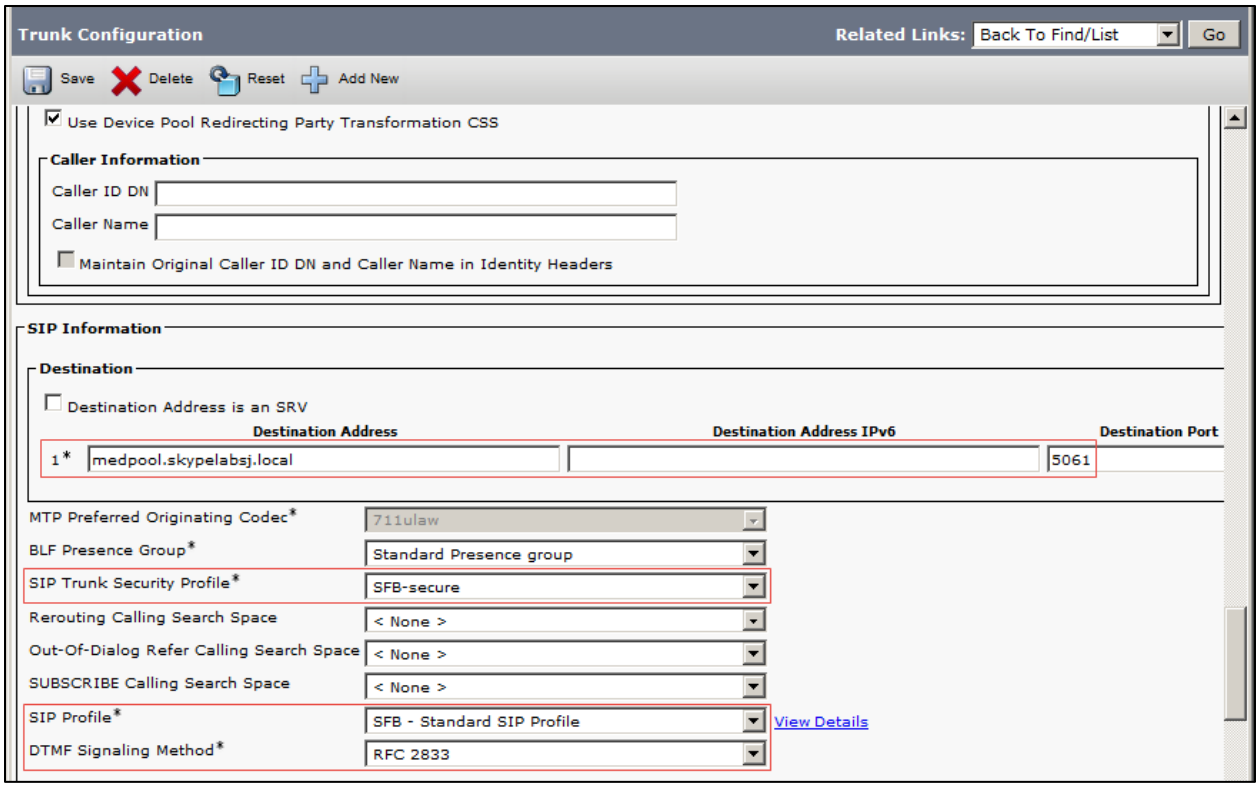
Cisco Unified Communications Manager SIP Trunk to Skype for Business Configuration (Continued)



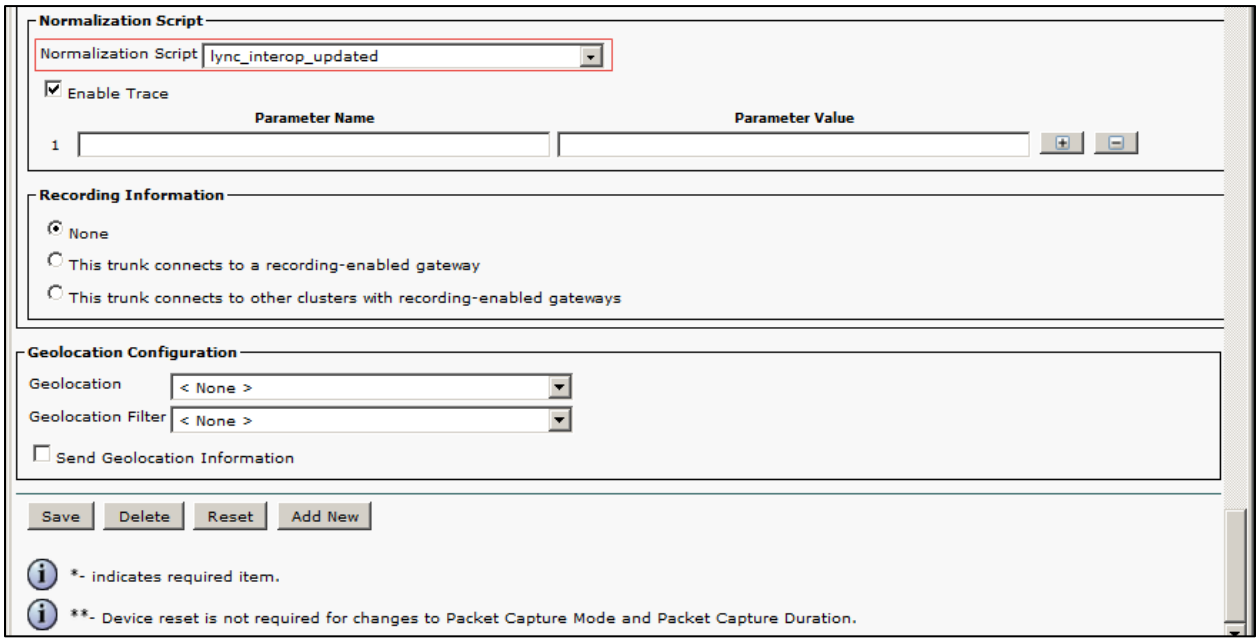
Cisco Unified Communications Manager SIP Trunk to Skype for Business Configuration (Continued)



Cisco Unified Communications Manager SIP Trunk to Skype for Business Configuration (Continued)



Cisco Unified Communications Manager SIP Trunk to Skype for Business Configuration (Continued)



Cisco Unified Communications Manager SIP Trunk to Cisco Unity Connection Configuration

Navigation: Device → Trunk

Set Device Name*= UnityConnection-TLS. This is used for the test.

Set Description = this text is used to identify this Trunk Group.

Set Device Pool* = G711 Preferred

Check Run On All Active Unified CM Nodes

Check Redirecting Diversion Header Delivery – Inbound

Check Redirecting Diversion Header Delivery – Outbound

Set Destination Address = 10.80.10.5. This is used for the test.

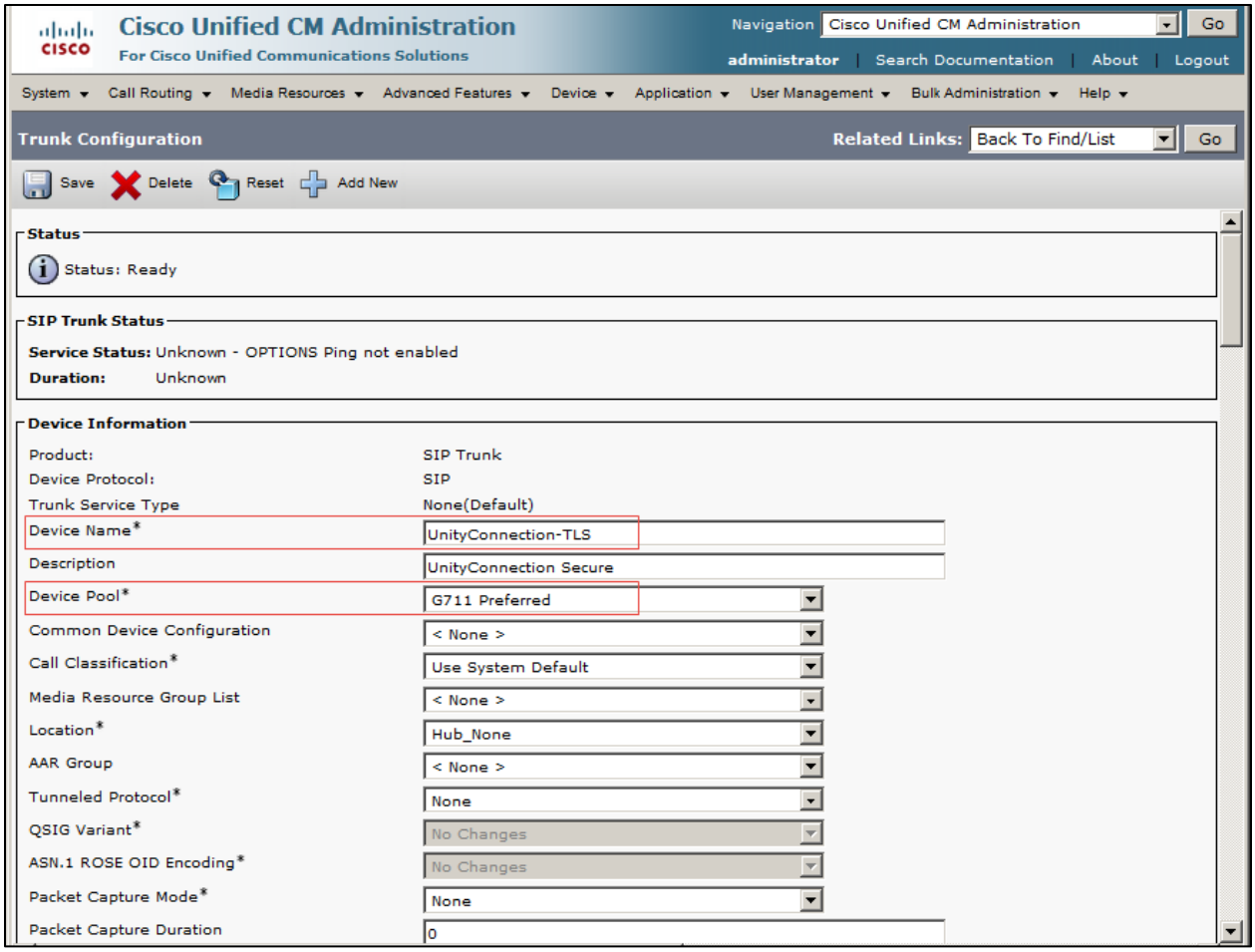
Set SIP Trunk Security Profile*= TLS_CUC

Set SIP Profile*= SFB-Standard SIP Profile

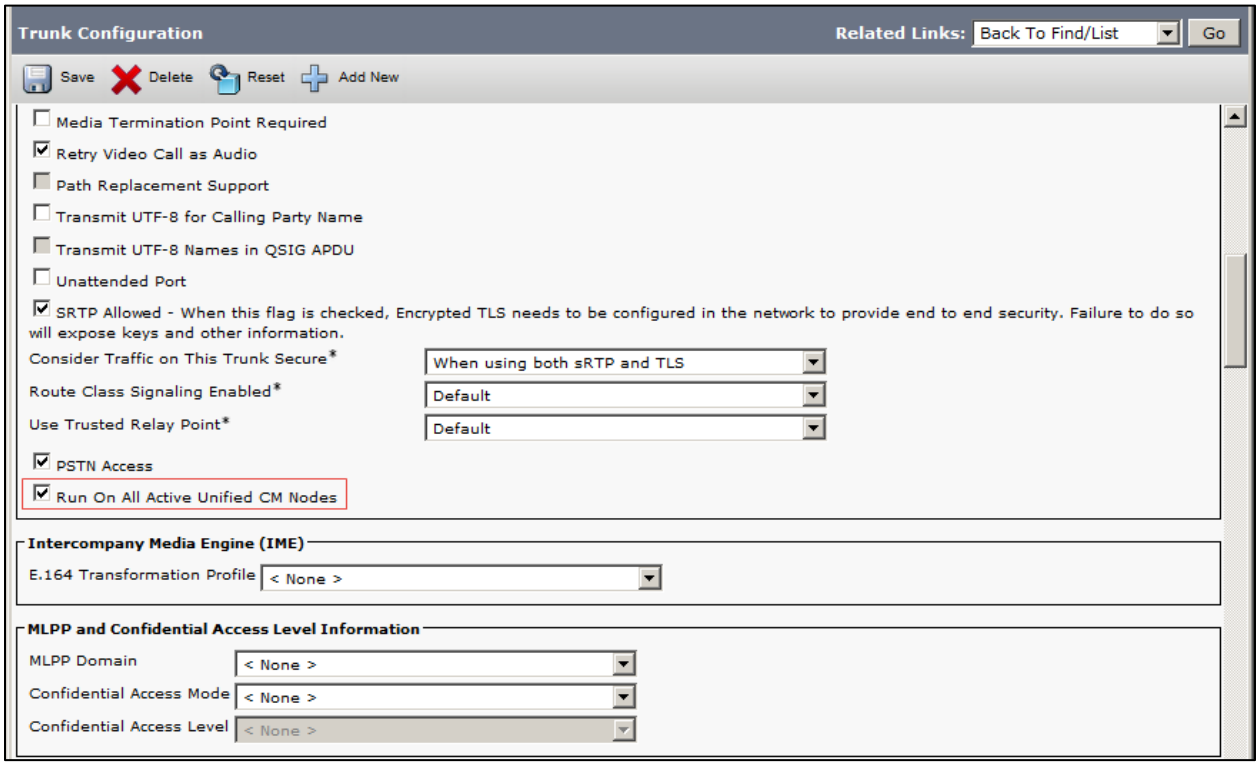
DTMF Signaling Method *= RFC 2833

Set Normalization Script = lync_interop_updated

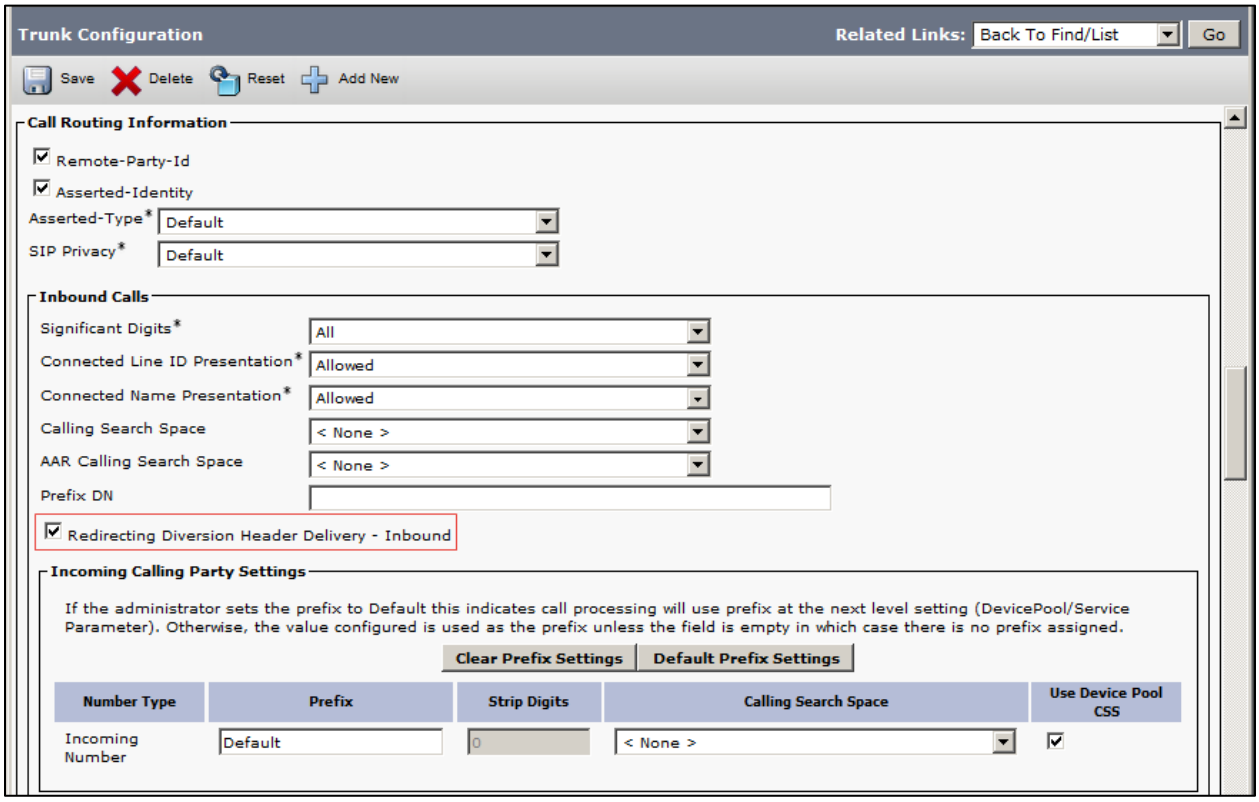
All other values are default



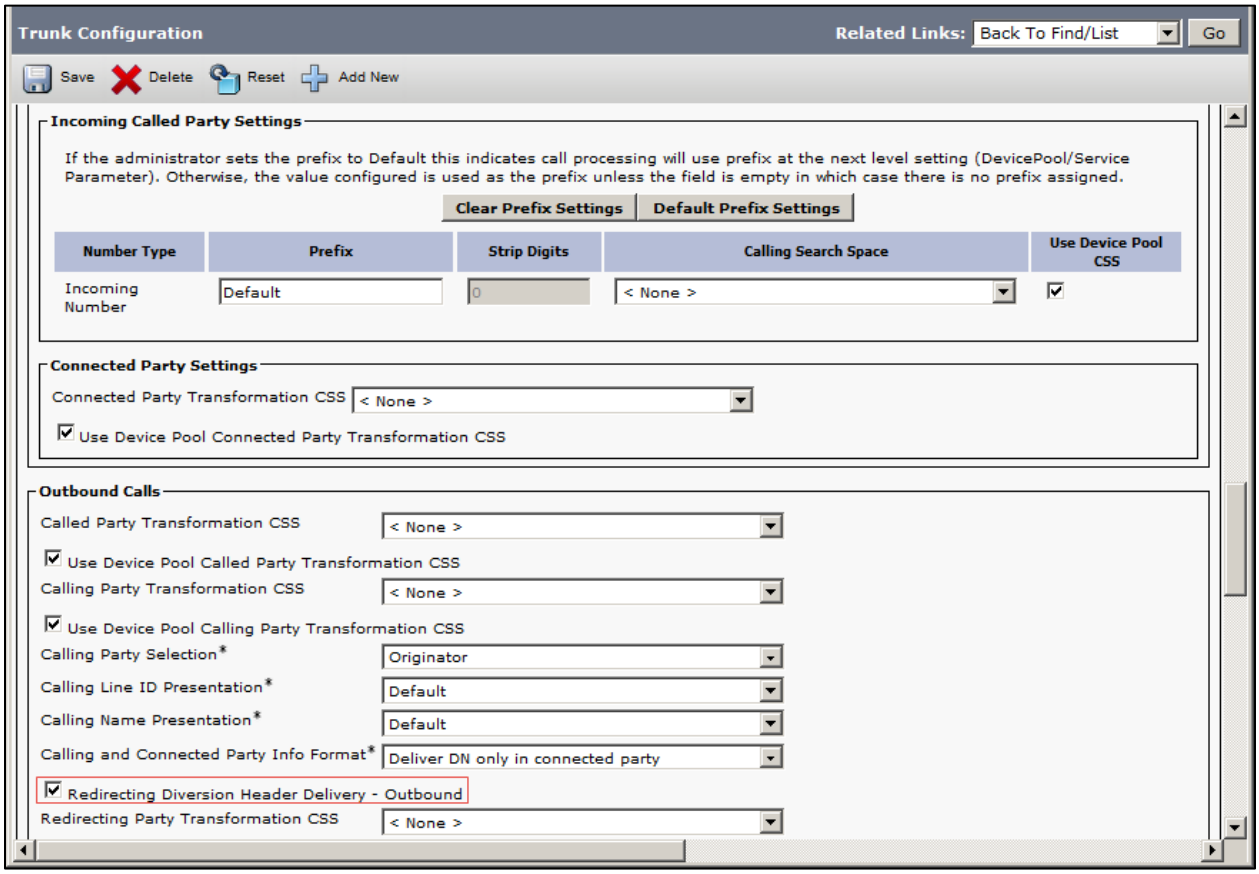
Cisco Unified Communications Manager SIP Trunk to Cisco Unity Connection Configuration (Continued)



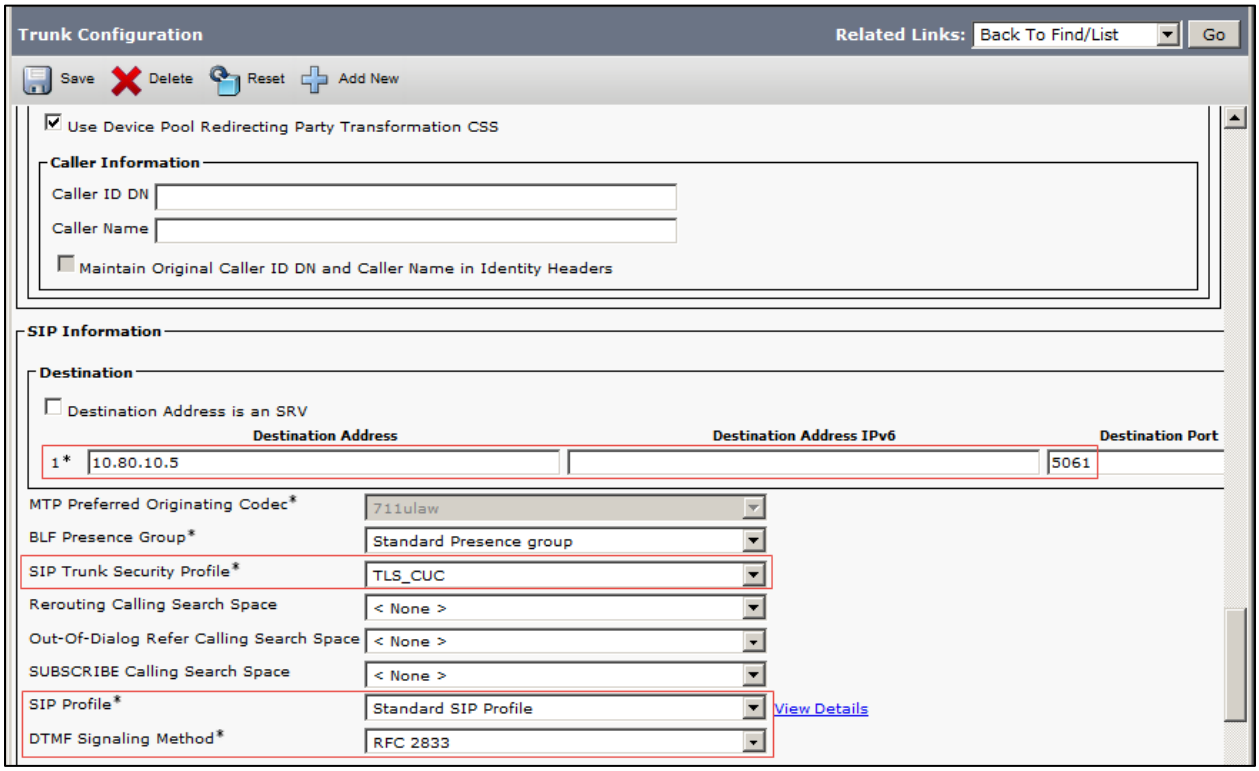
Cisco Unified Communications Manager SIP Trunk to Cisco Unity Connection Configuration (Continued)



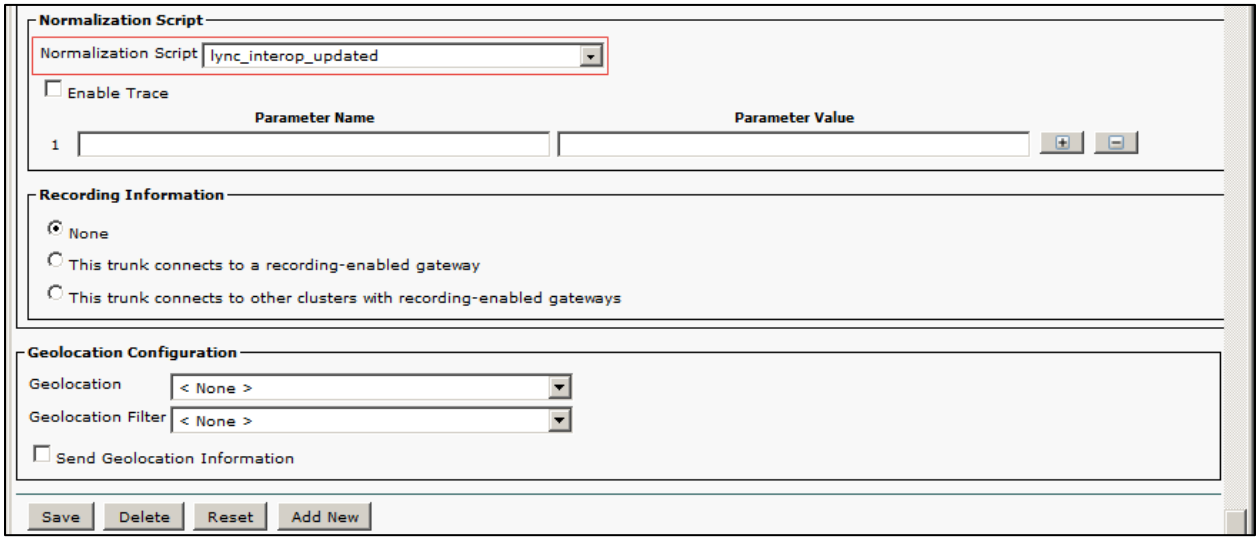
Cisco Unified Communications Manager SIP Trunk to Cisco Unity Connection Configuration (Continued)



Cisco Unified Communications Manager SIP Trunk to Cisco Unity Connection Configuration (Continued)



Cisco Unified Communications Manager SIP Trunk to Cisco Unity Connection Configuration (Continued)



Cisco Unified Communications Manager Route Group

Navigation: Call Routing → Route/Hunt → Route Group

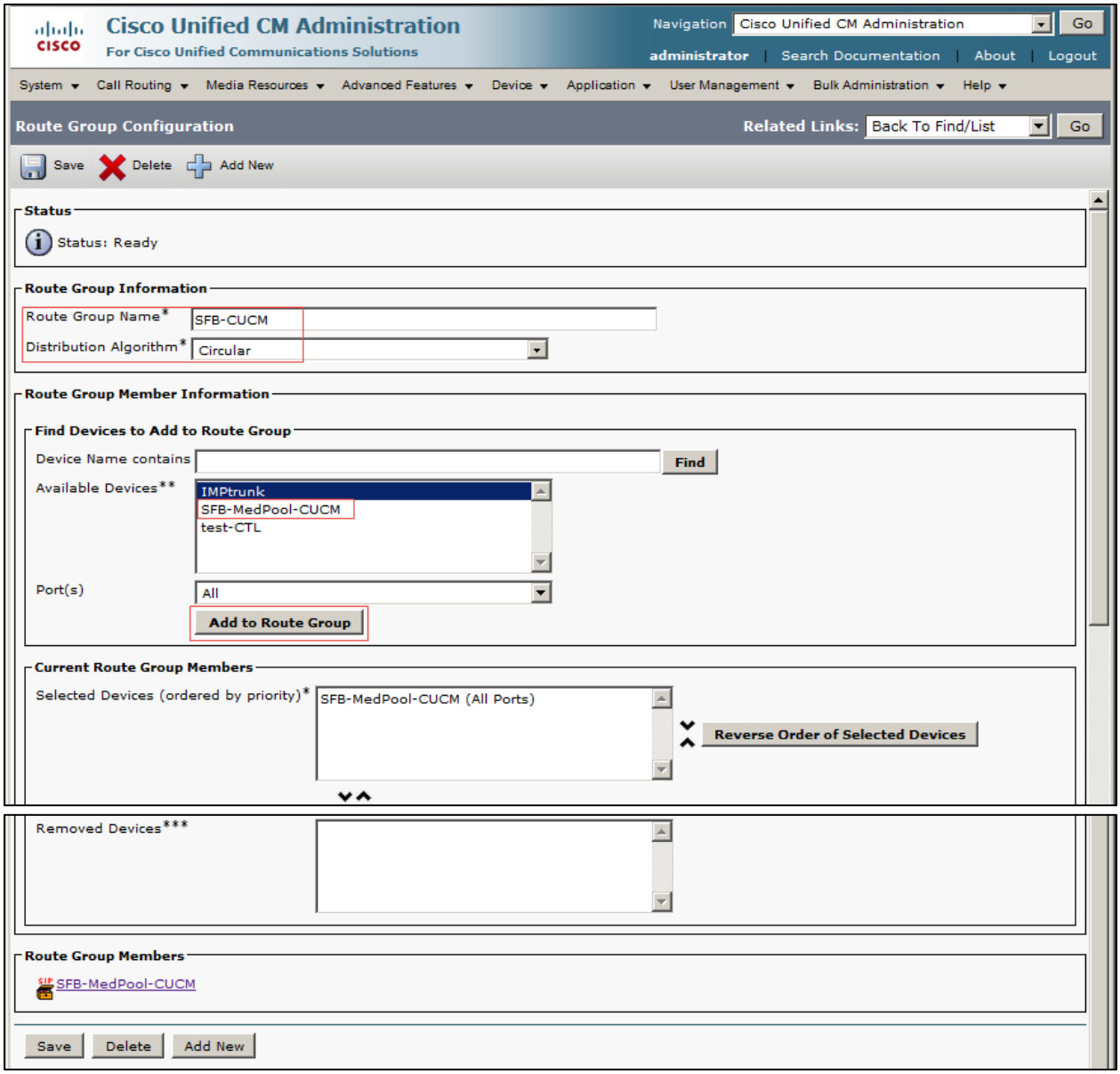
Add New

SFB-CUCM was configured in this test

Set Route Group Name = SFB-CUCM

Set Distribution Algorithm = Circular

Select SFB-MedPool-CUCM from Available Devices and click the Add to Route Group



Cisco Unified Communications Manager Route List

Navigation: Call Routing → Route/Hunt → Route List

Add New

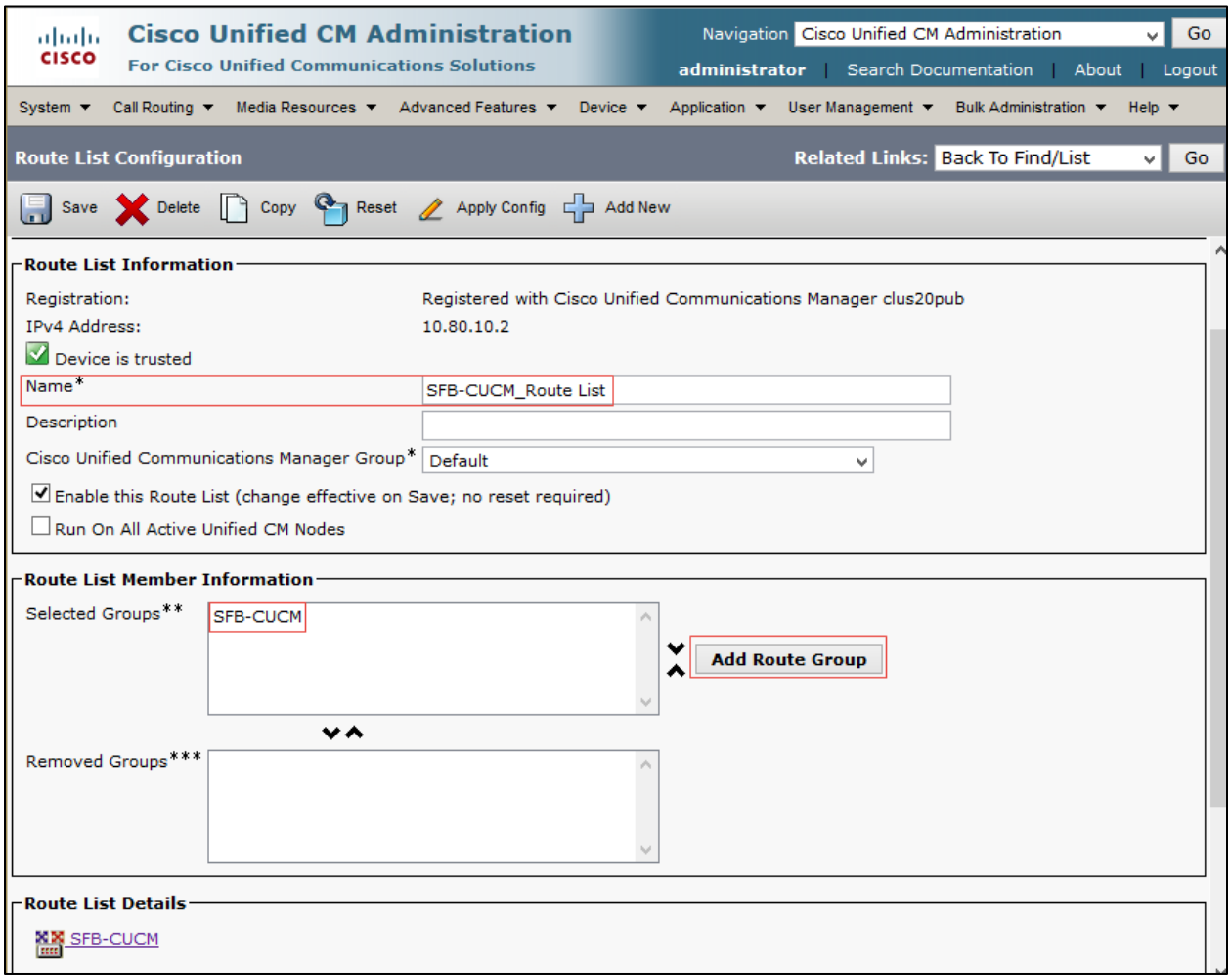
SFB-CUCM_Route List was created for this test.

Set Name: SFB-CUCM_Route List

Set Cisco Unified Communications Manager Group = Default

Click on Add Route Group

Set Route Group* = SFB-CUCM-[NON-QSIG]



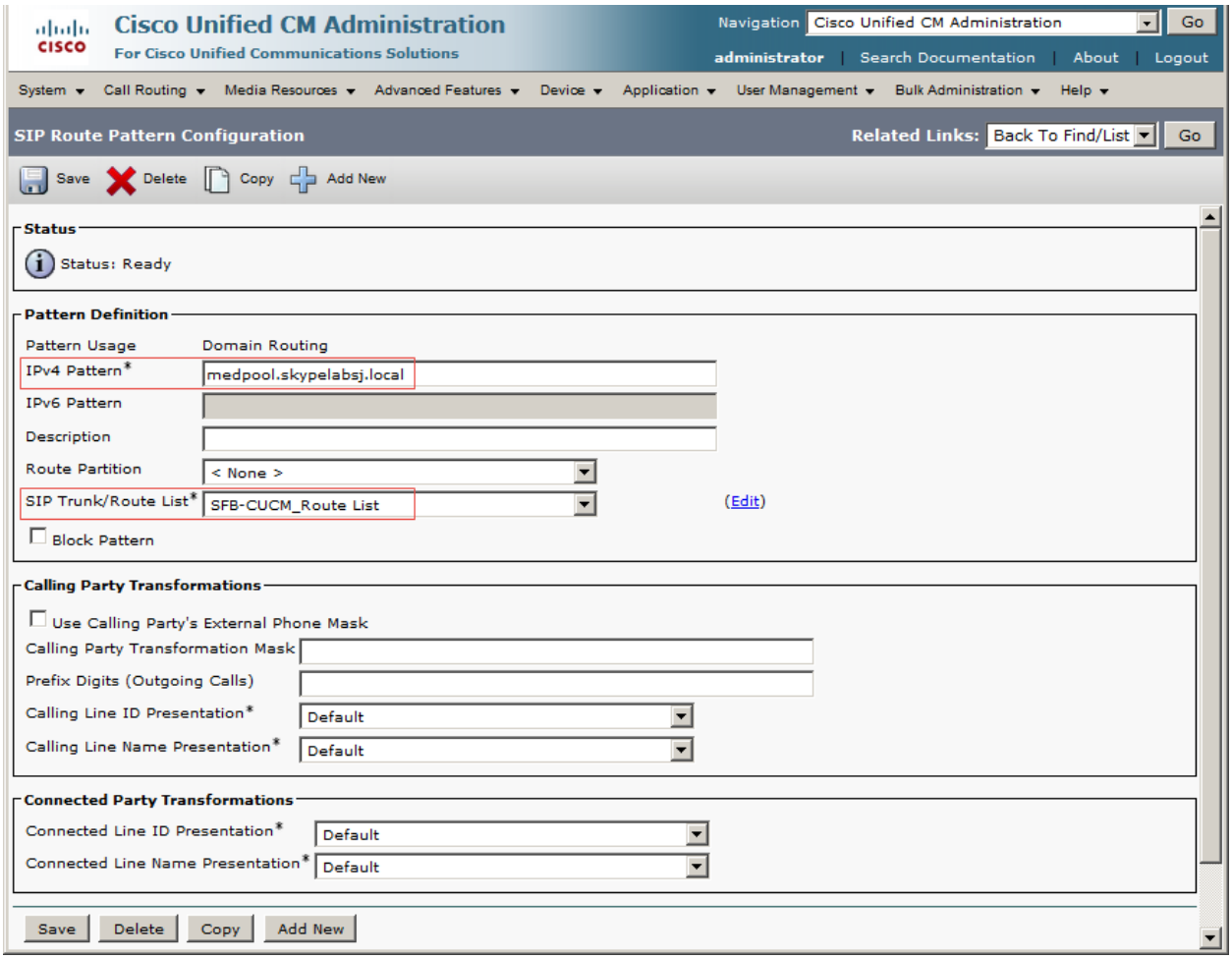
Cisco Unified Communications Manager SIP Route Pattern

Navigation: Call Routing → SIP Route Pattern

Add New

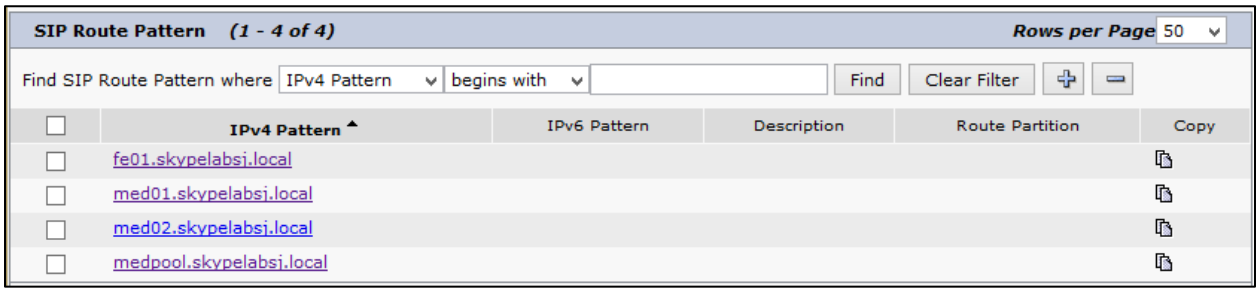
Set IPv4 Pattern* = medpool.skypelabsj.local. This is the FQDN of the Skype for Business Front End server.

Set SIP Trunk/Route List* = SFB_CUCM_Route List



In a similar way, add SIP Route Patterns for all the servers that comprise the Skype for Business environment.

In the test, the following SIP Route Patterns were configured:



Cisco Unified Communications Manager Voice Mail Configuration

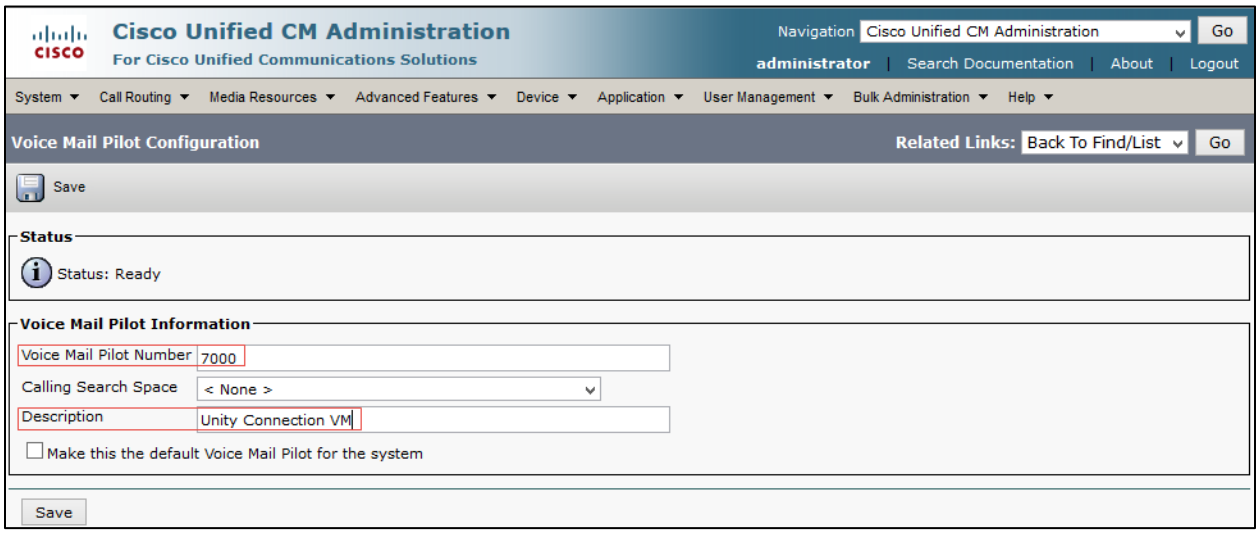
Configure Voice Mail Pilot:

Navigation: Advanced Features → Voice Mail → Voice Mail Pilot

Add new

Set Voice Mail Pilot Number = 7000 .This is used for the test

Set Description = Unity Connection VM .This text is used to identify this SIP Profile



Cisco Unified Communications Manager Route Pattern to Skype for Business Extensions

Navigation: Call Routing → Route/Hunt → Route Pattern

Add New

Set Route Pattern* = 8XXX. This is used to route to the Skype for Business in this test

Set Description = this text is used to identify this Route Pattern

Set Gateway/Route List* = SFB-CUCM_Route List. This is used for the test

Uncheck Provide Outside Dial Tone

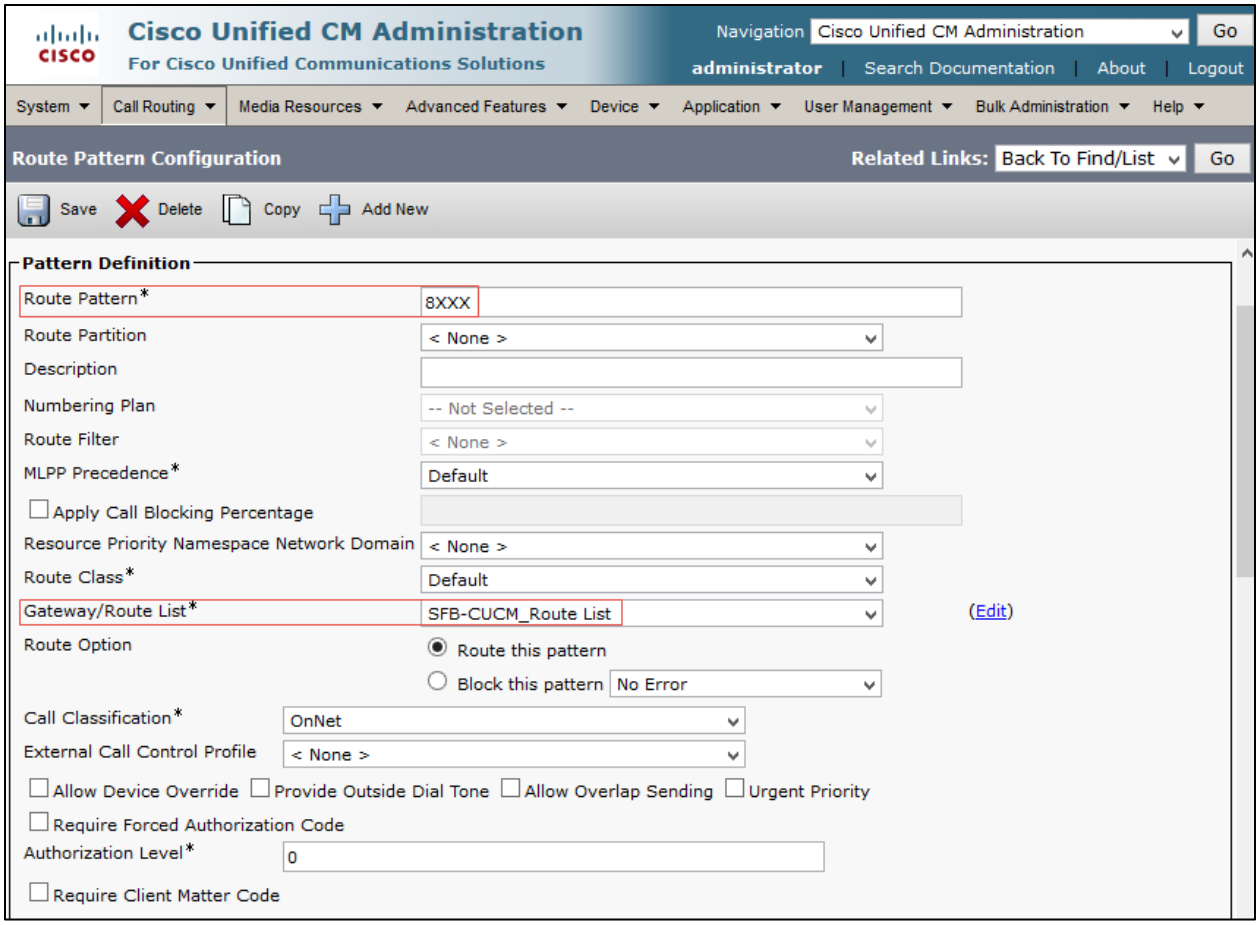
Set Calling Line ID Presentation= Default

Set Calling Name Presentation= Default

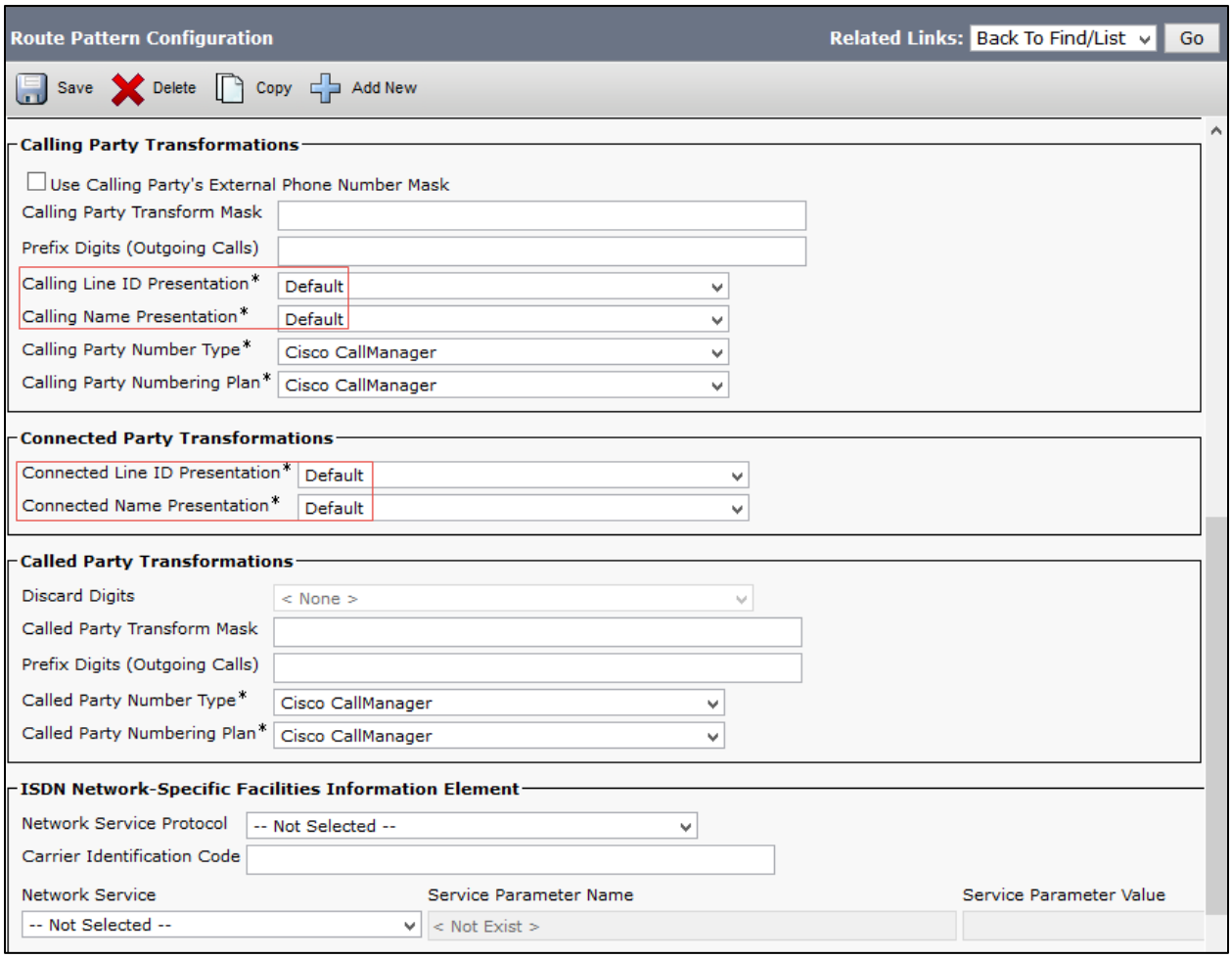
Set Connected Line ID Presentation*= Default

Set Calling Name Presentation* = Default

All other values are default.



Route Pattern Configuration for 8xxx (Continued)



Cisco Unified Communications Manager Route Pattern to invoke Jabber client with Remote Destination configured as Skype for Business Extensions

Set Route Pattern* = \+.8XXX. This is used to route to the Skype for Business when using the Extend and Connect functionality in this test

Set Description = this text is used to identify this Route Pattern

Set Gateway/Route List* = SFB-CUCM_Route List. This is used for the test

Uncheck Provide Outside Dial Tone

Set Calling Line ID Presentation= Default

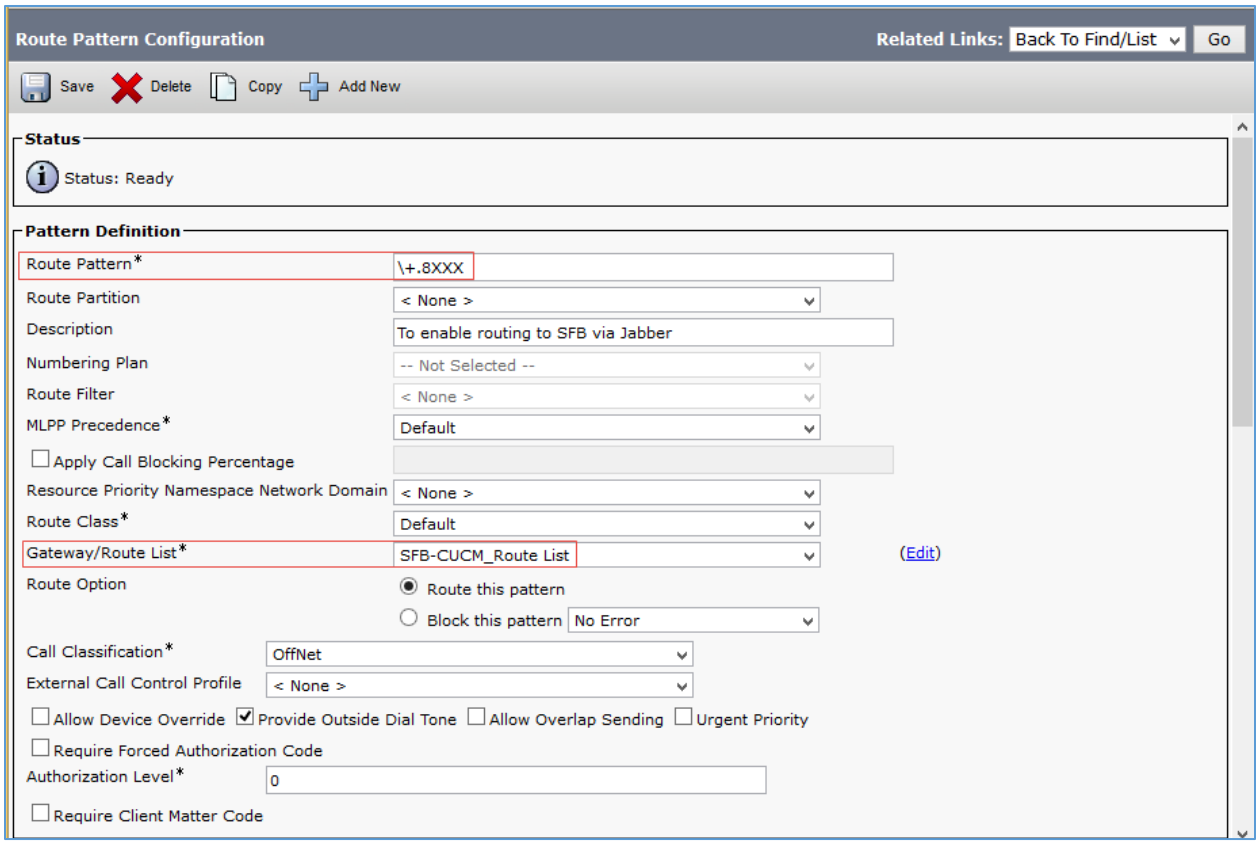
Set Calling Name Presentation= Default

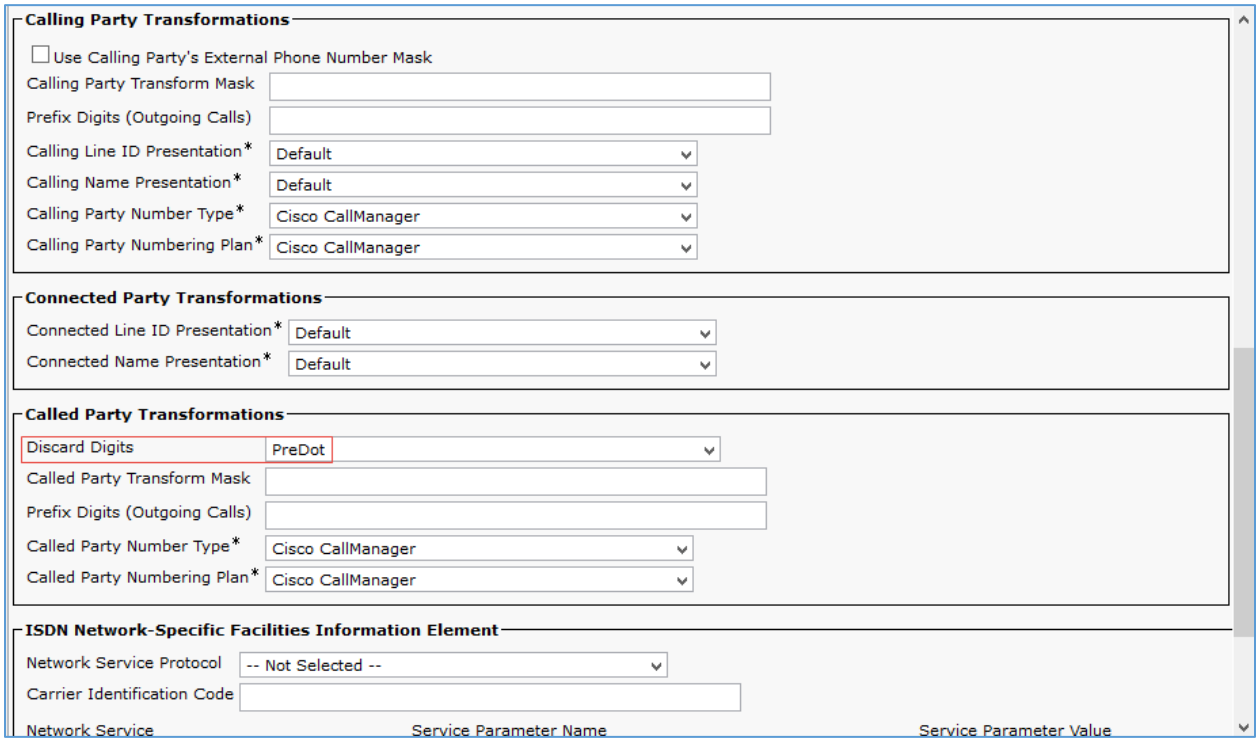
Set Connected Line ID Presentation*= Default

Set Calling Name Presentation* = Default

Discard Digits = PreDot

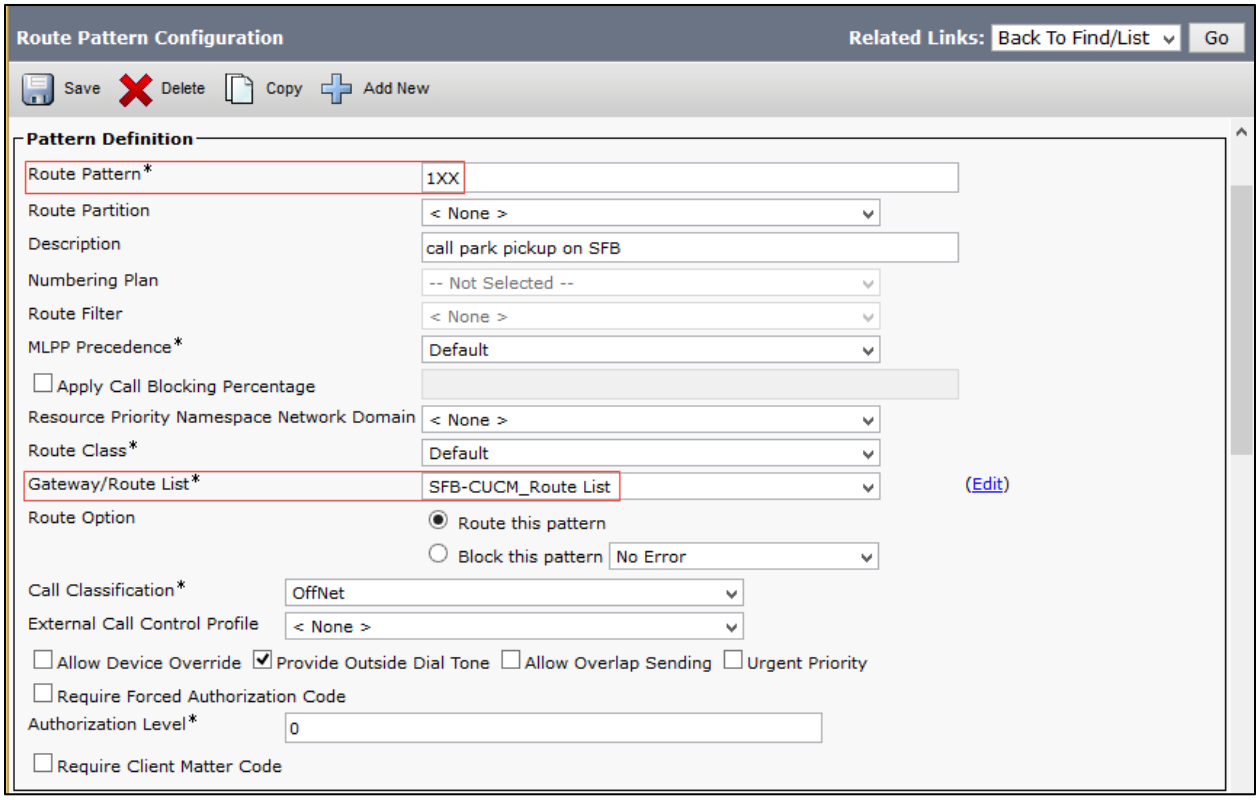
All other values are default



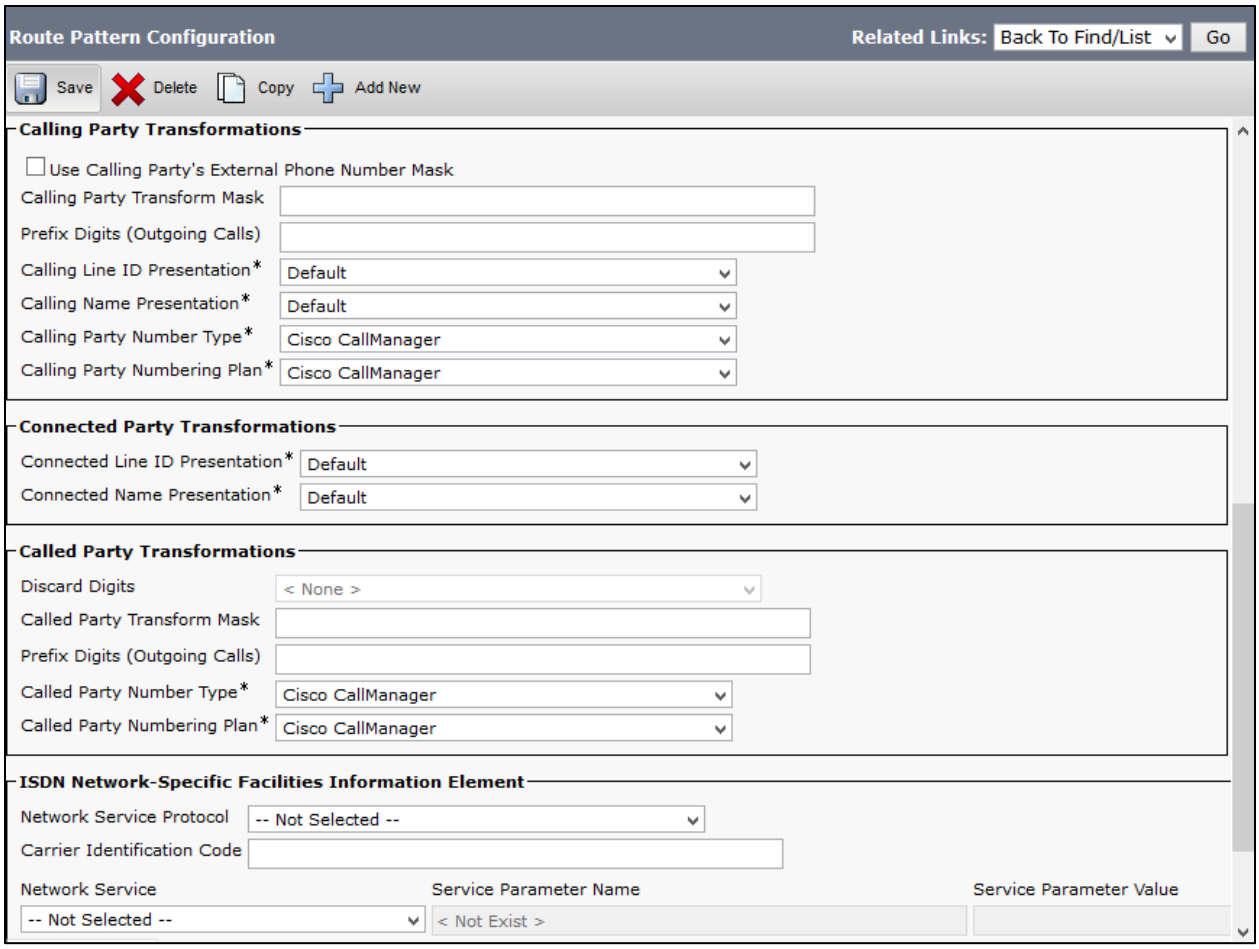


Cisco Unified Communications Manager Route Pattern to Skype for Business Call Park range

The Skype for Business Call Park range configured is 100-199 .The following route pattern “1XX” is therefore configured to enable a parked call to be retrieved from Cisco UCM.

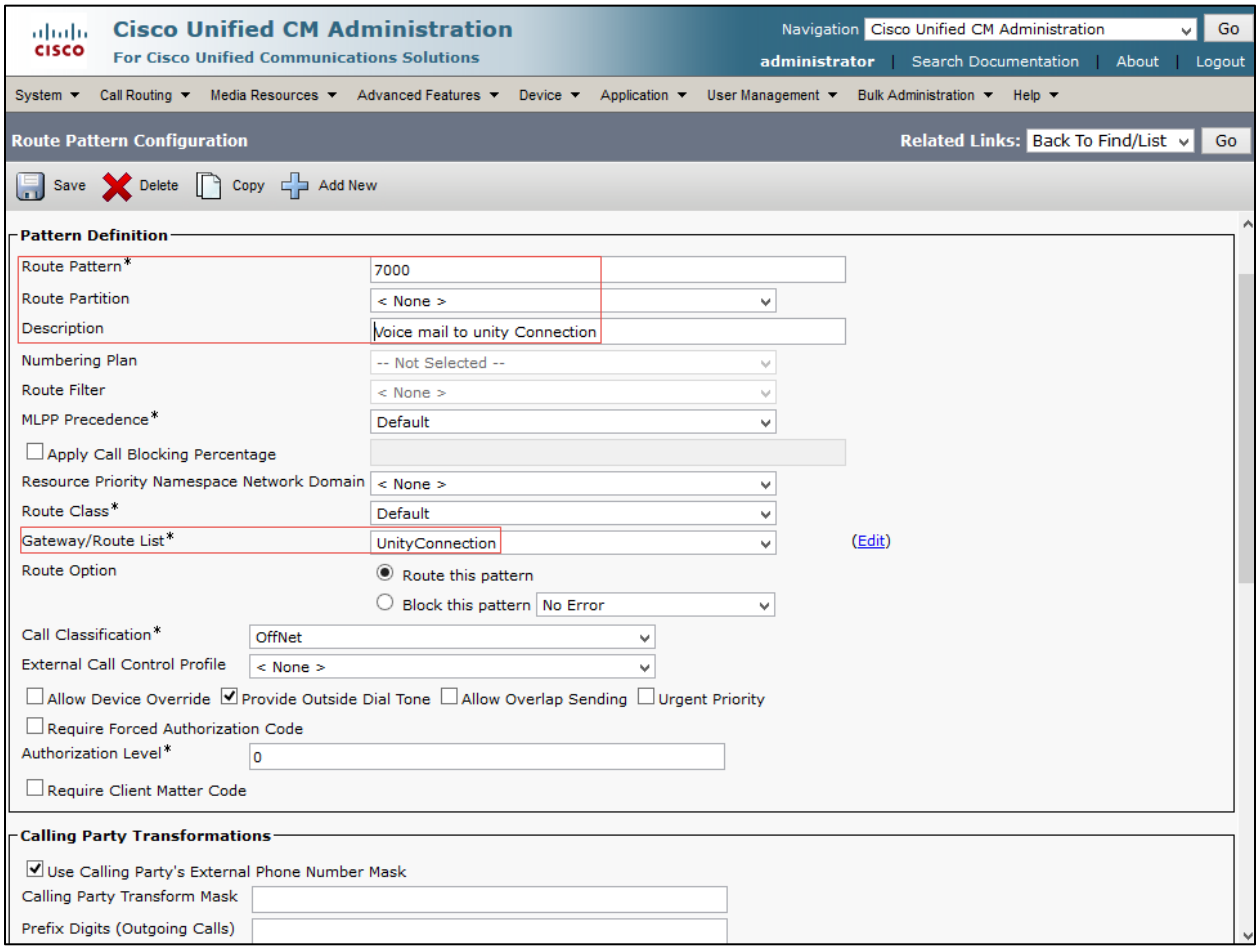


Route Pattern Configuration for 1XX (Continued)

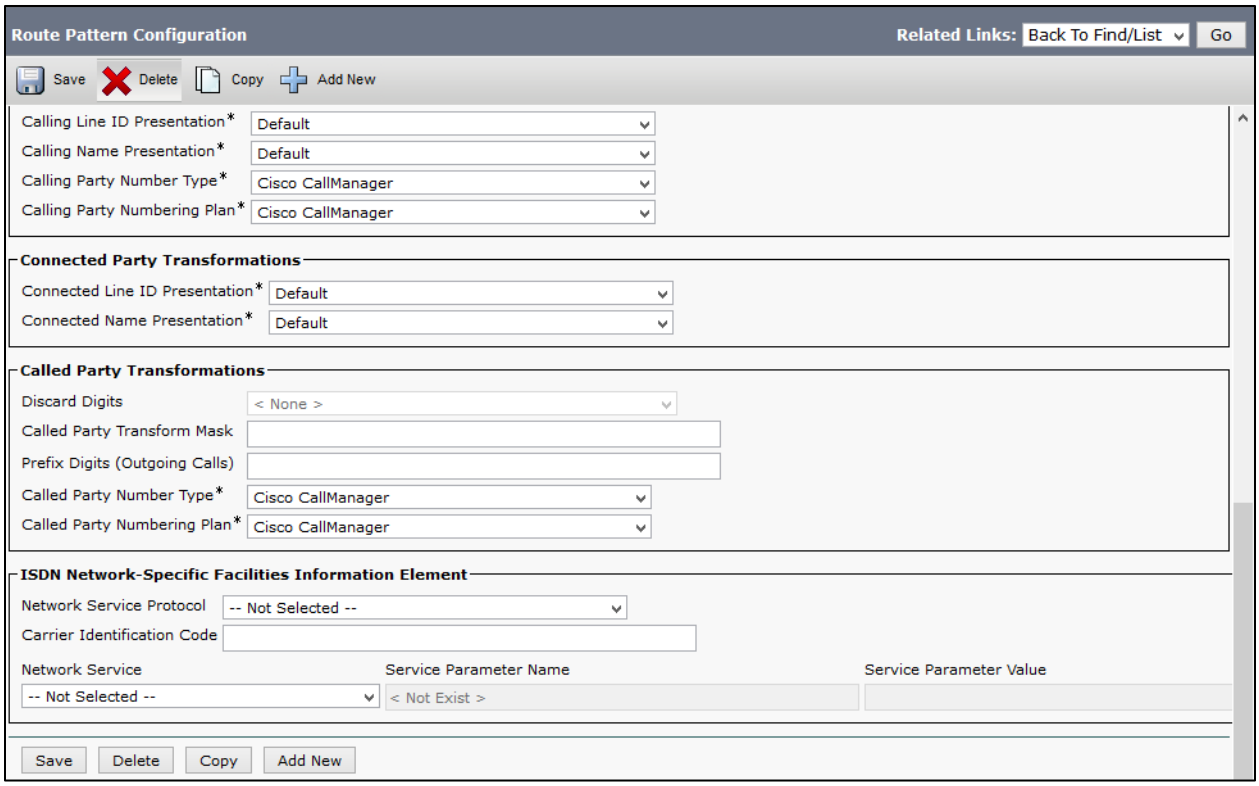


Cisco Unified Communications Manager Route Pattern to Unity Connection Voice Mail

A route pattern 7000 (which is the voice mail pilot), is configured to reach Unity Connection Voice Mail.



Route Pattern Configuration for 7000 (Continued)



Cisco UCM Extent and Connect

Extend and Connect is a feature that allows administrators to rapidly deploy UC Computer Telephony Integration (CTI) applications which interoperate with any endpoint. With Extend and Connect, users can leverage the benefits of UC applications from any location using any device. This feature also allows Interoperability between newer UC solutions and legacy systems, so customers can migrate to newer UC Solutions over time as existing hardware is deprecated.

Cisco UCM UC service Configuration

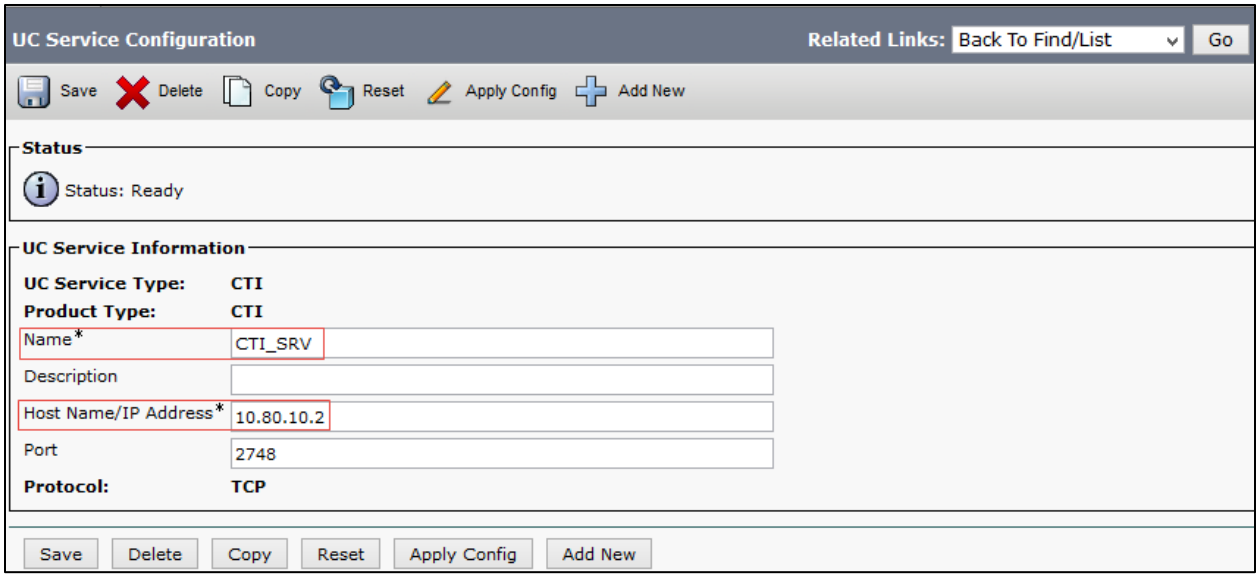
Navigation Path: User Management→ User setting → UC Service

Add New

Select Service Type as CTI

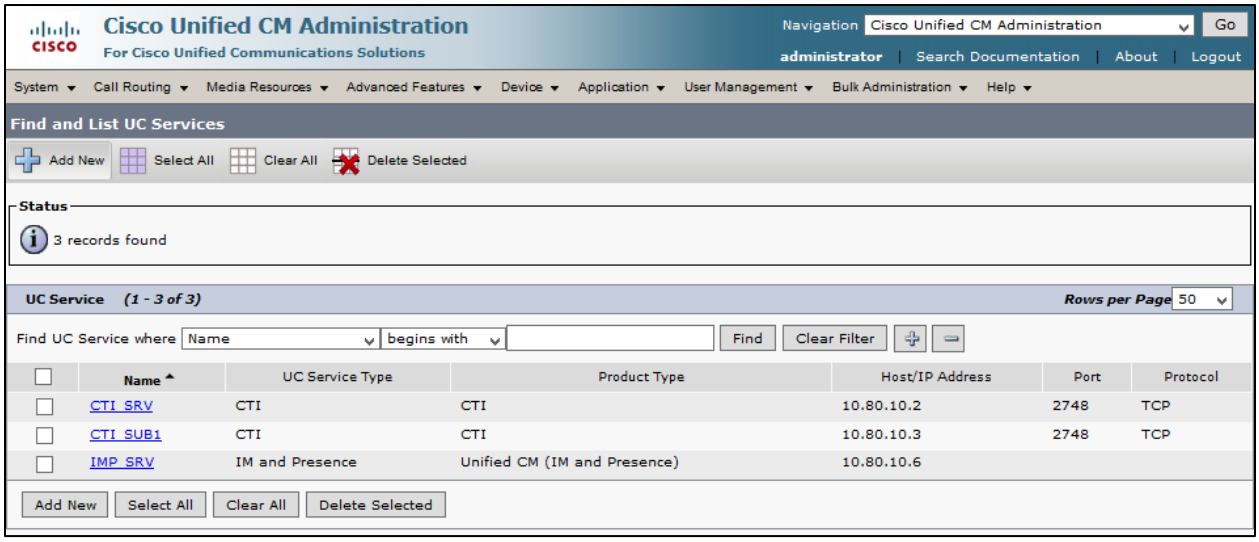
Set Name = CTI_SRV

Set Host Name/IP Address* = 10.80.10.2; this is the Cisco UCM publisher IP.



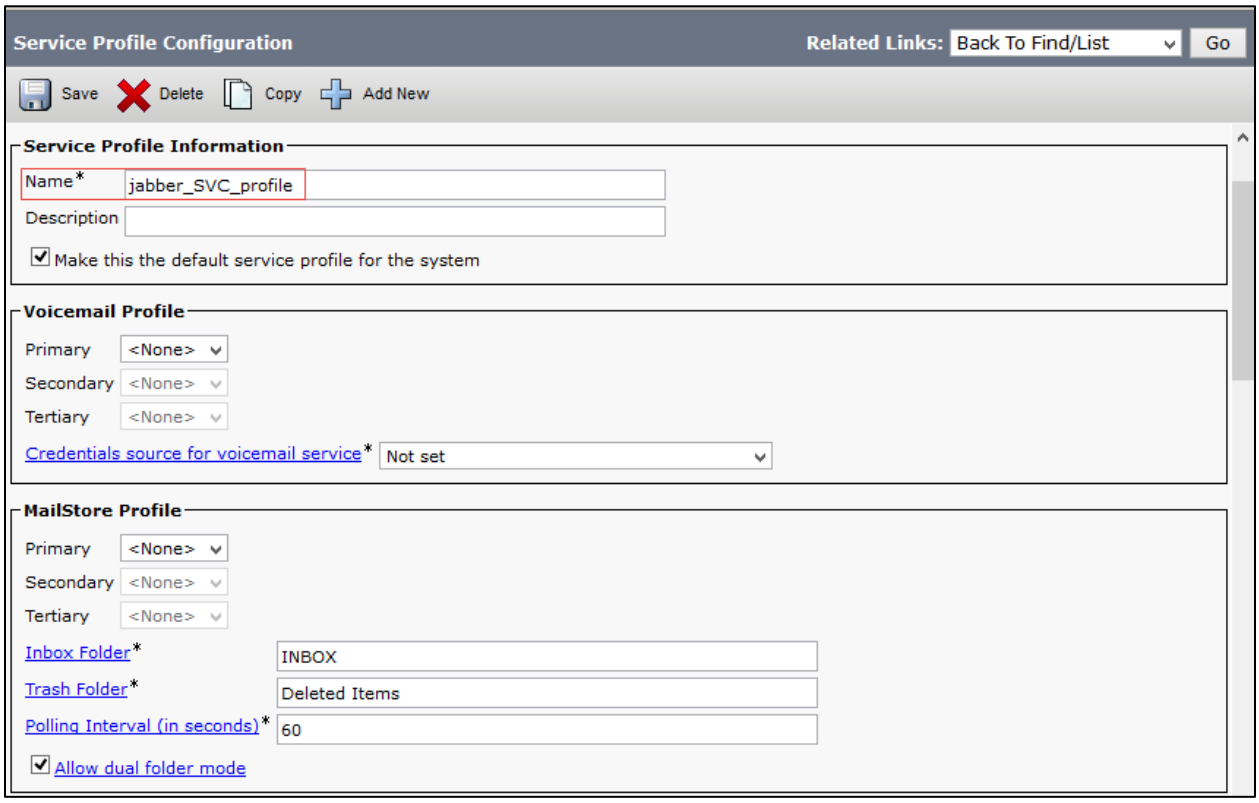
In the same manner, a UC Service is configured for the subscriber also.

A UC service of Type IM and Presence is configured with the IP of the Presence server.

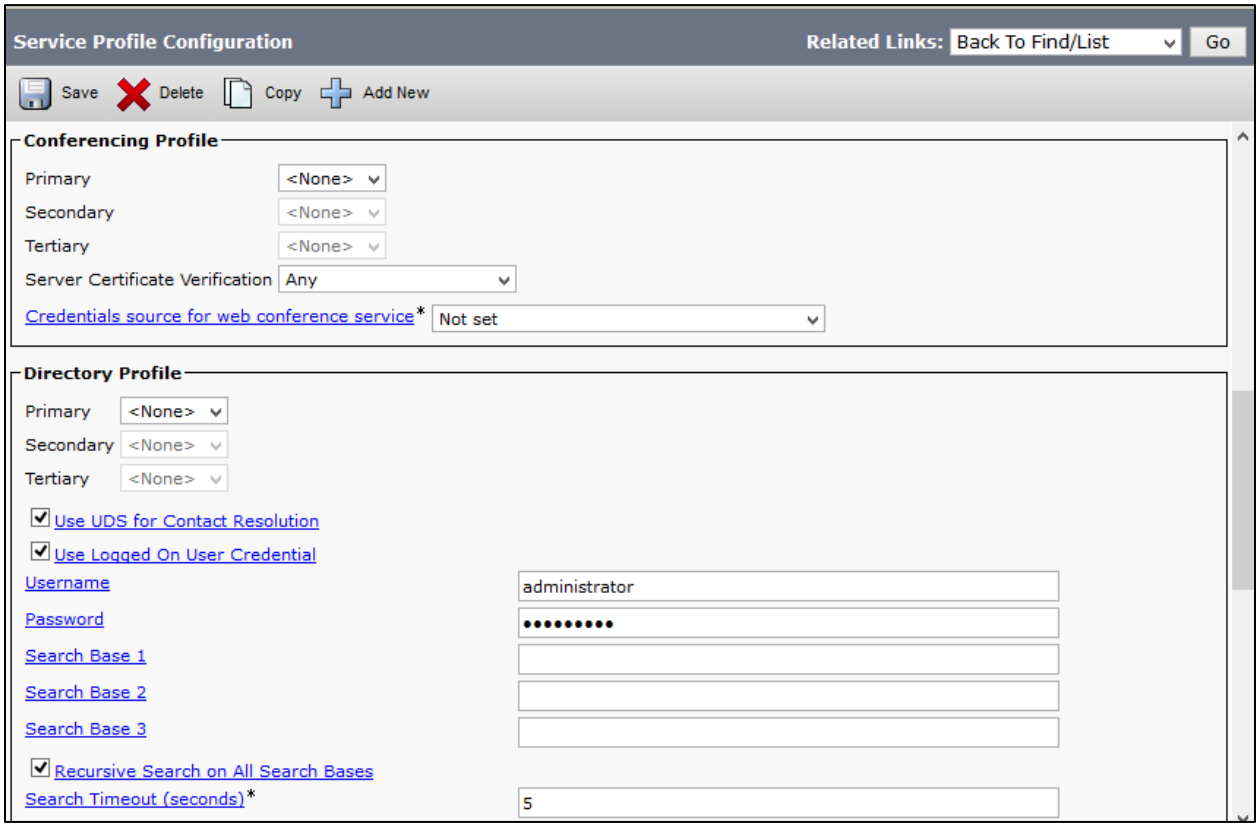


Cisco UCM service Profile Configuration

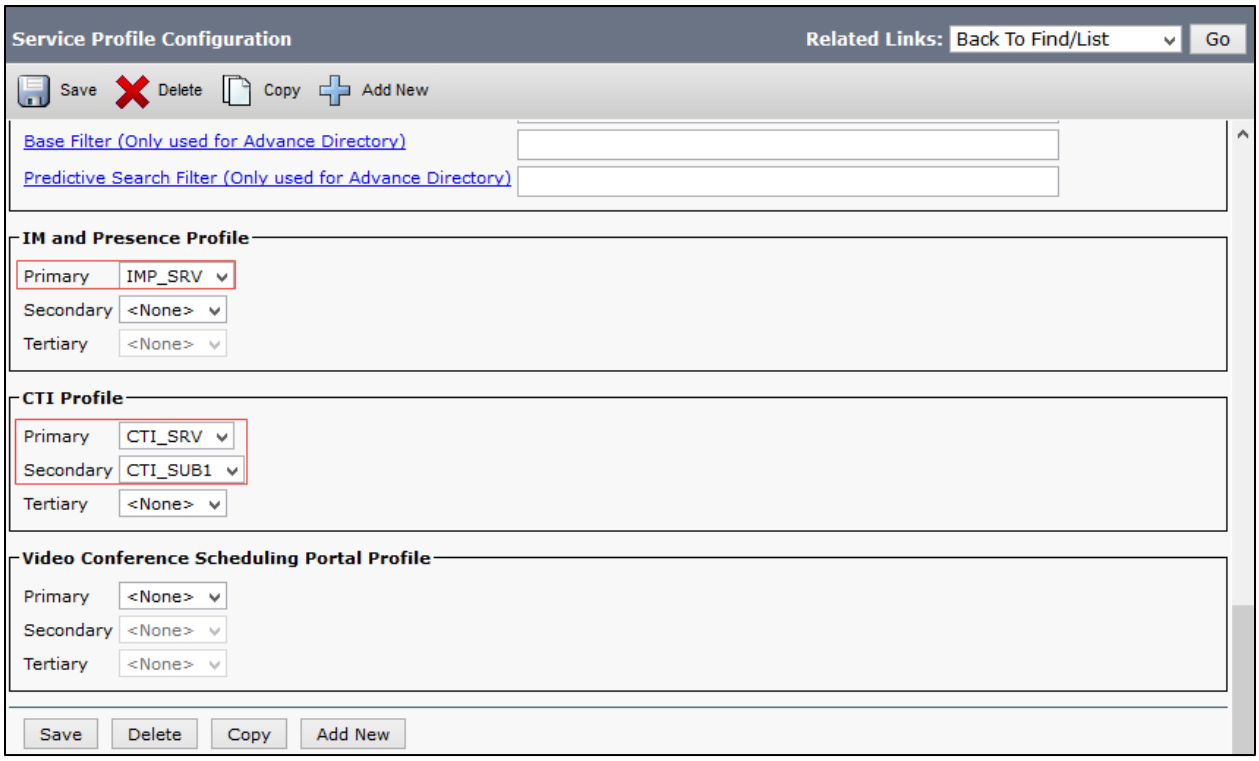
Navigation: User Management→ User setting → Service Profile



Cisco UCM service profile Configuration (Continued)



Cisco UCM service profile Configuration (Continued)



Cisco Unified CM IM Presence – CCMCIP Profile Configuration

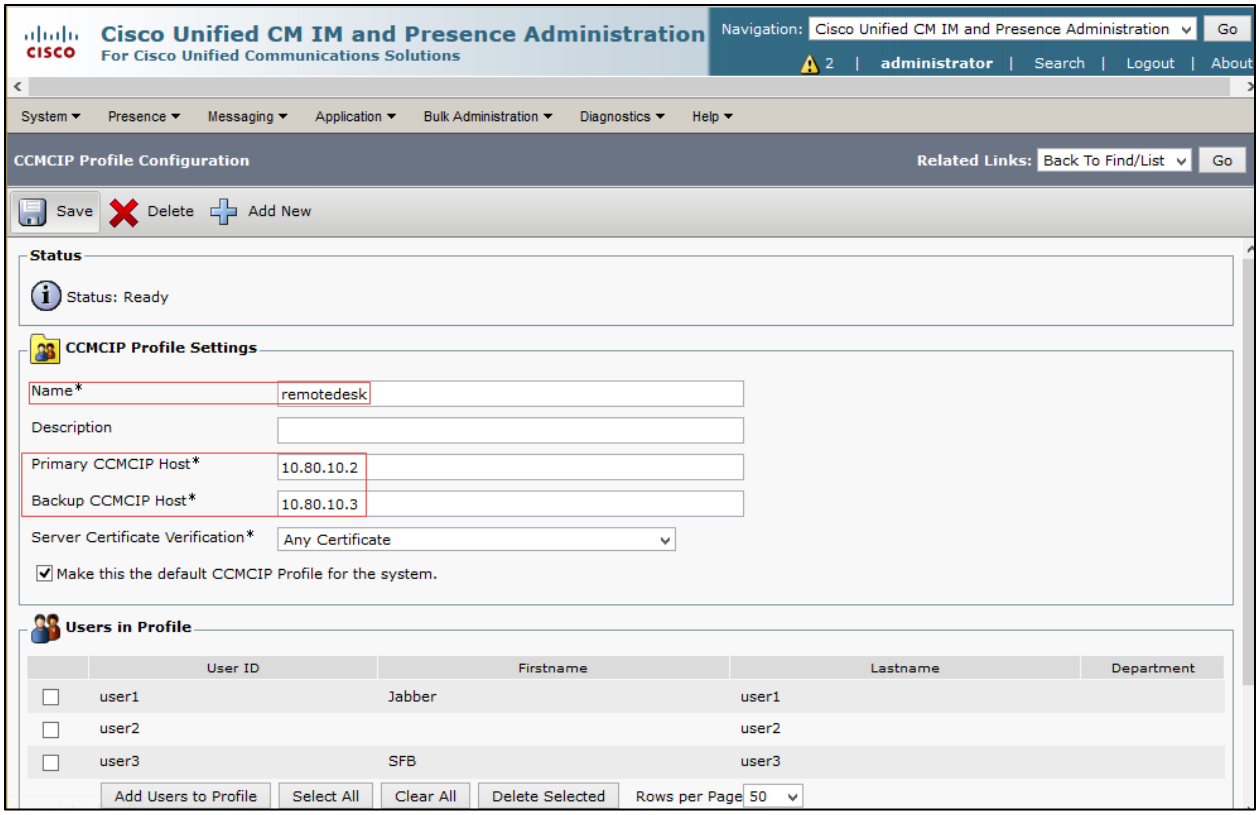
Navigation Path: Application → CCMCIP Profile

Set Name *: remotedesk. This is used in this example.

Set Primary CCMCIP Host *: 10.80.10.2.Cisco Publisher IP. This is used in this test.

Set Backup CCMCIP Host *: 10.80.10.3.Cisco Publisher IP. This is used in this test.

Add Users to Profile: user1, user 2 and user3 .This is used in this test.



Cisco UCM – SIP trunk to Cisco IM&Presence Trunk Configuration

Navigation Path: Device→ Trunk

Set Device Name*= IMPTrunk. This is used for the test.

Set Description = this text is used to identify this Trunk Group.

Set Device Pool* = Default. This is used for the test.

Set Media Resource Group List = MRGL. This is used for the test.

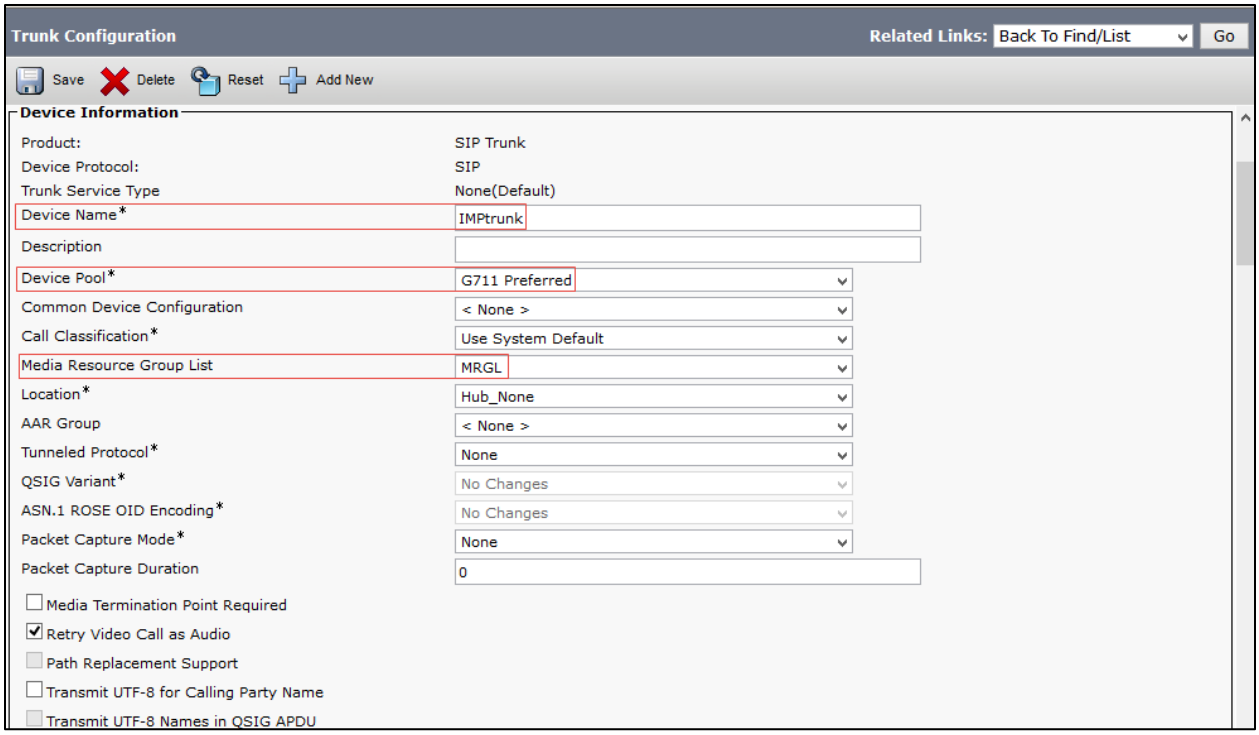
Set Destination Address = 10.80.10.6. This is used in this example.

Set SIP Trunk Security Profile*= Non Secure SIP Trunk Profile.

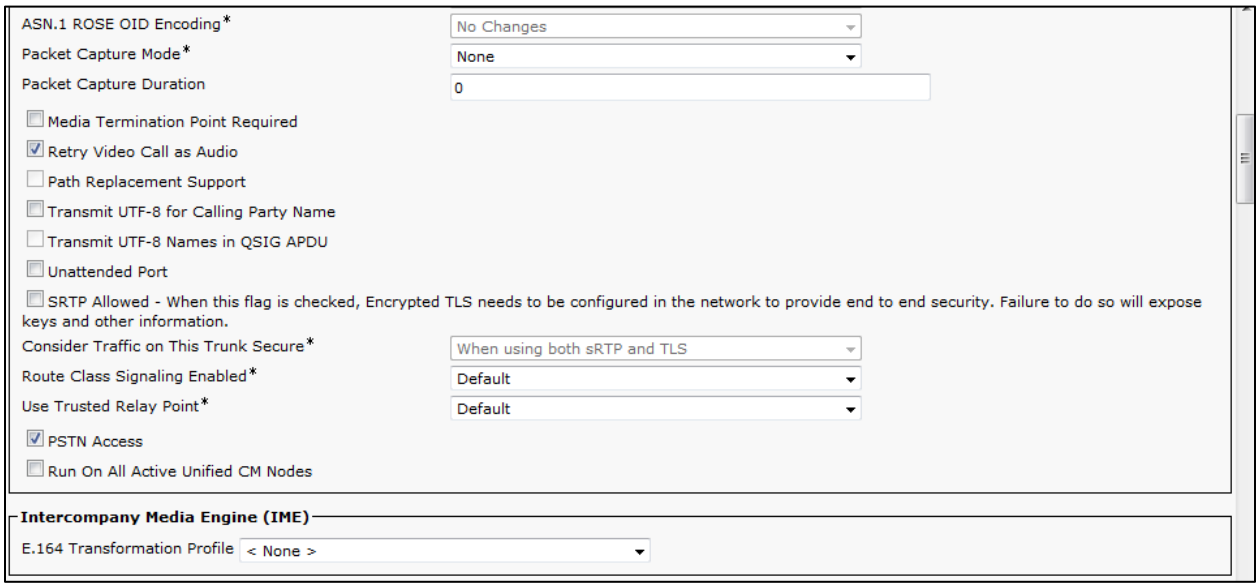
Set SIP Profile*= Standard SIP Profile.

Set DTMF Signaling Method*= No Preference.

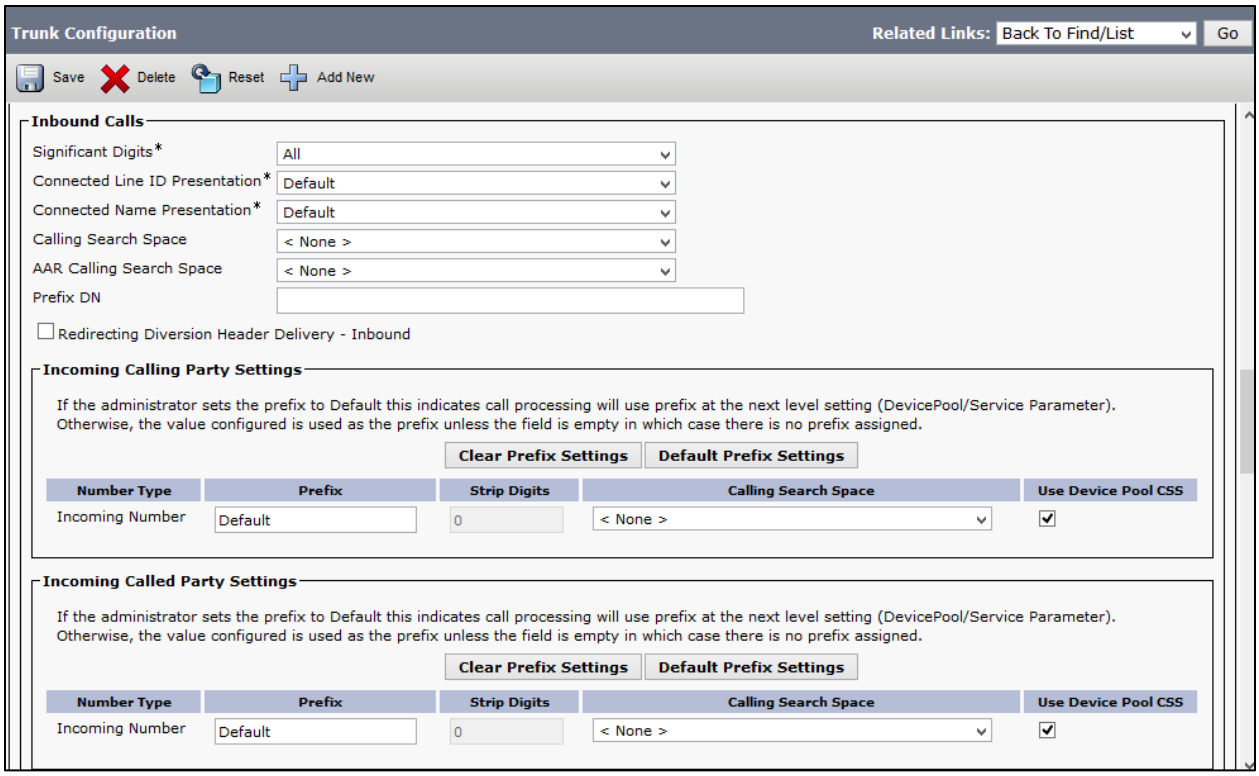
All other values are default.



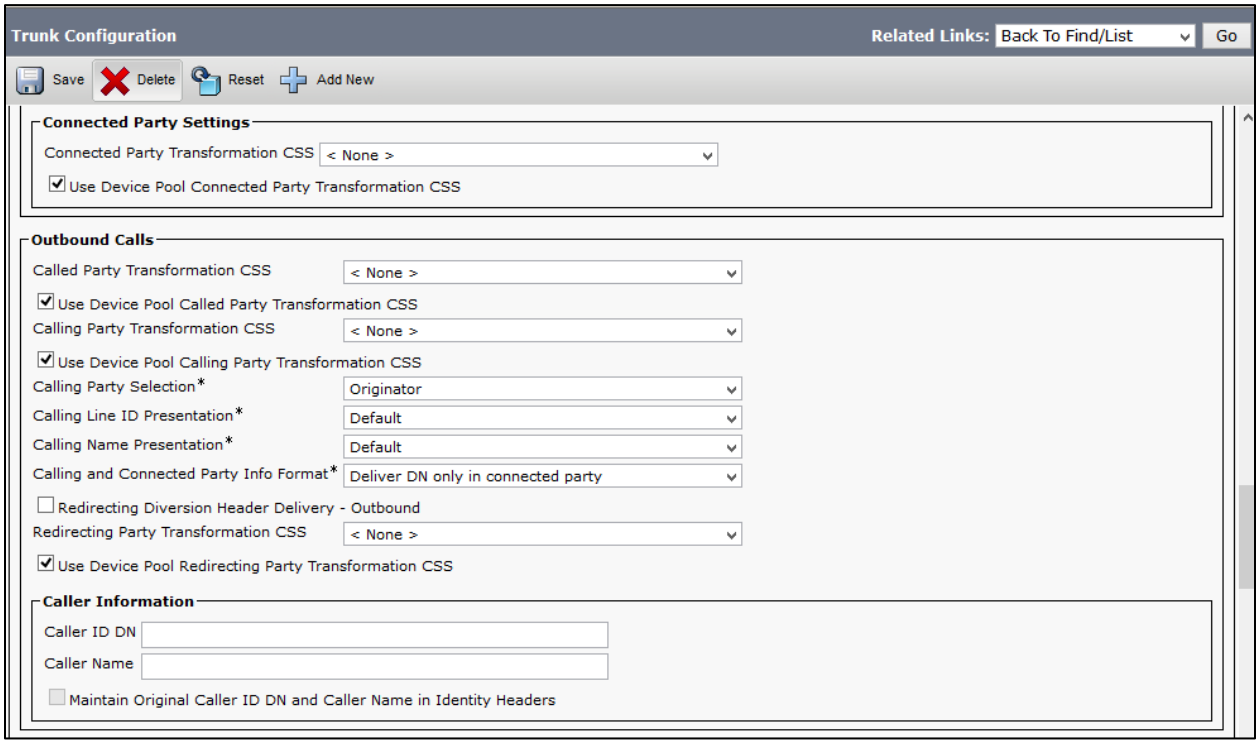
Cisco Unified Communications Manager SIP Trunk to CUP Configuration (Continued)



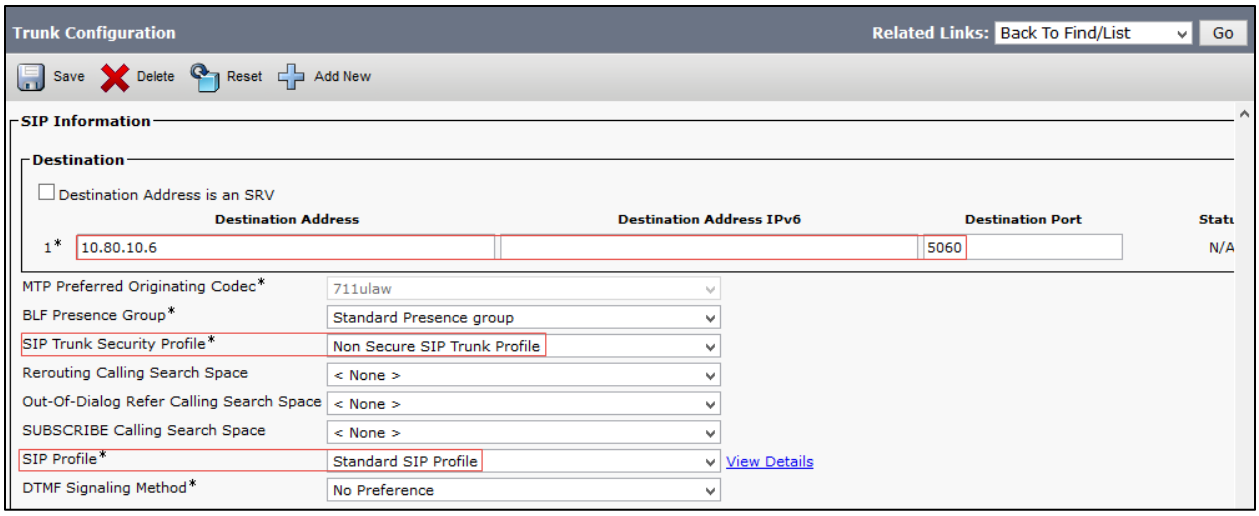
Cisco UCM SIP Trunk to CUP Configuration (Continued)



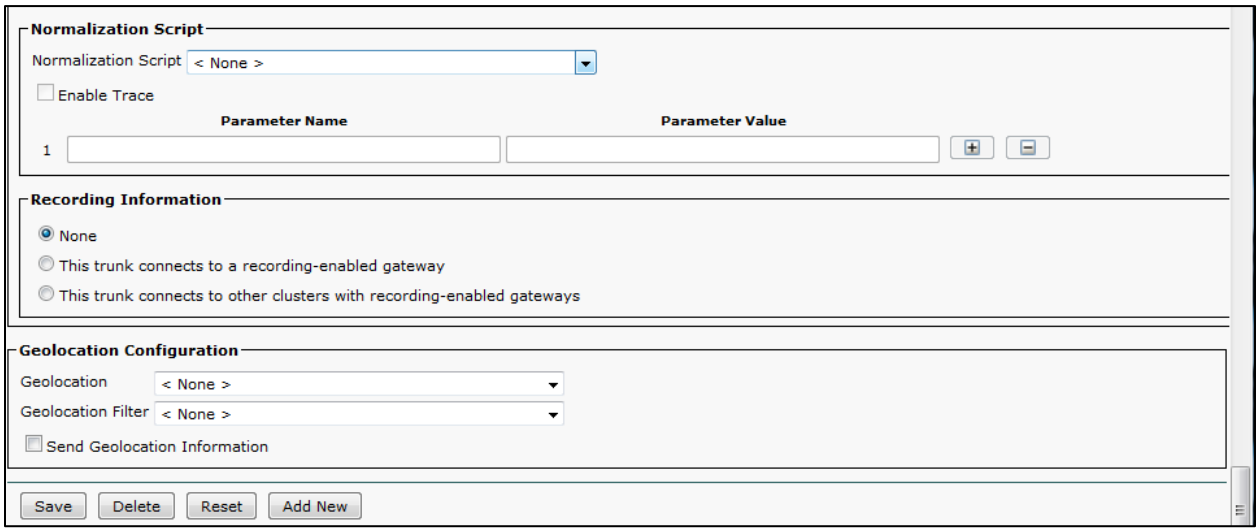
Cisco UCM SIP Trunk to CUP Configuration (Continued)



Cisco UCM SIP Trunk to CUP Configuration (Continued)



Cisco UCM SIP Trunk to CUP Configuration (Continued)



Cisco UCM end user configuration

Add user to Cisco UCM

Navigation: User Management→ End user

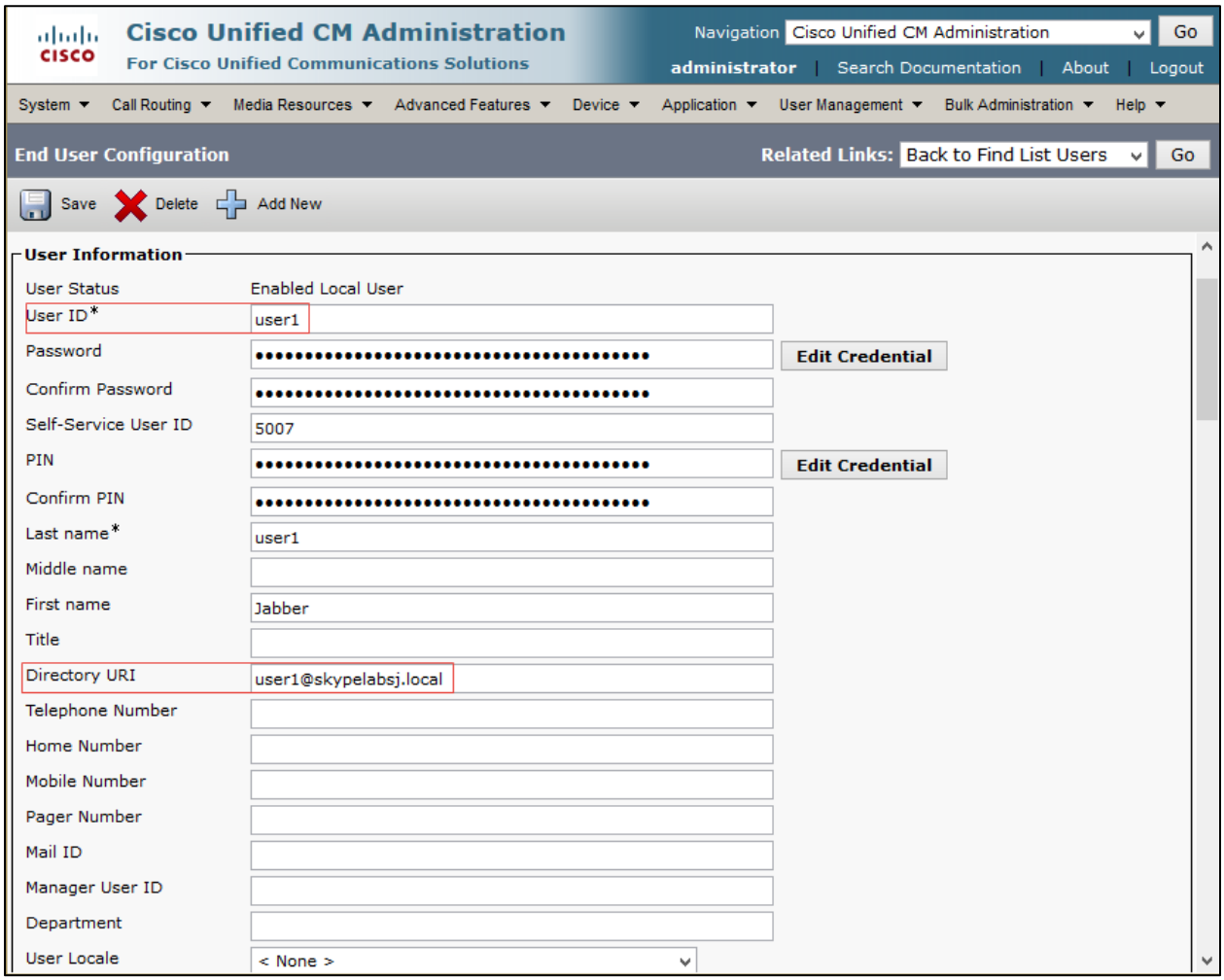
Set User ID*= user1. This is used for the test.

Set Last Name = user1. This is used for the test.

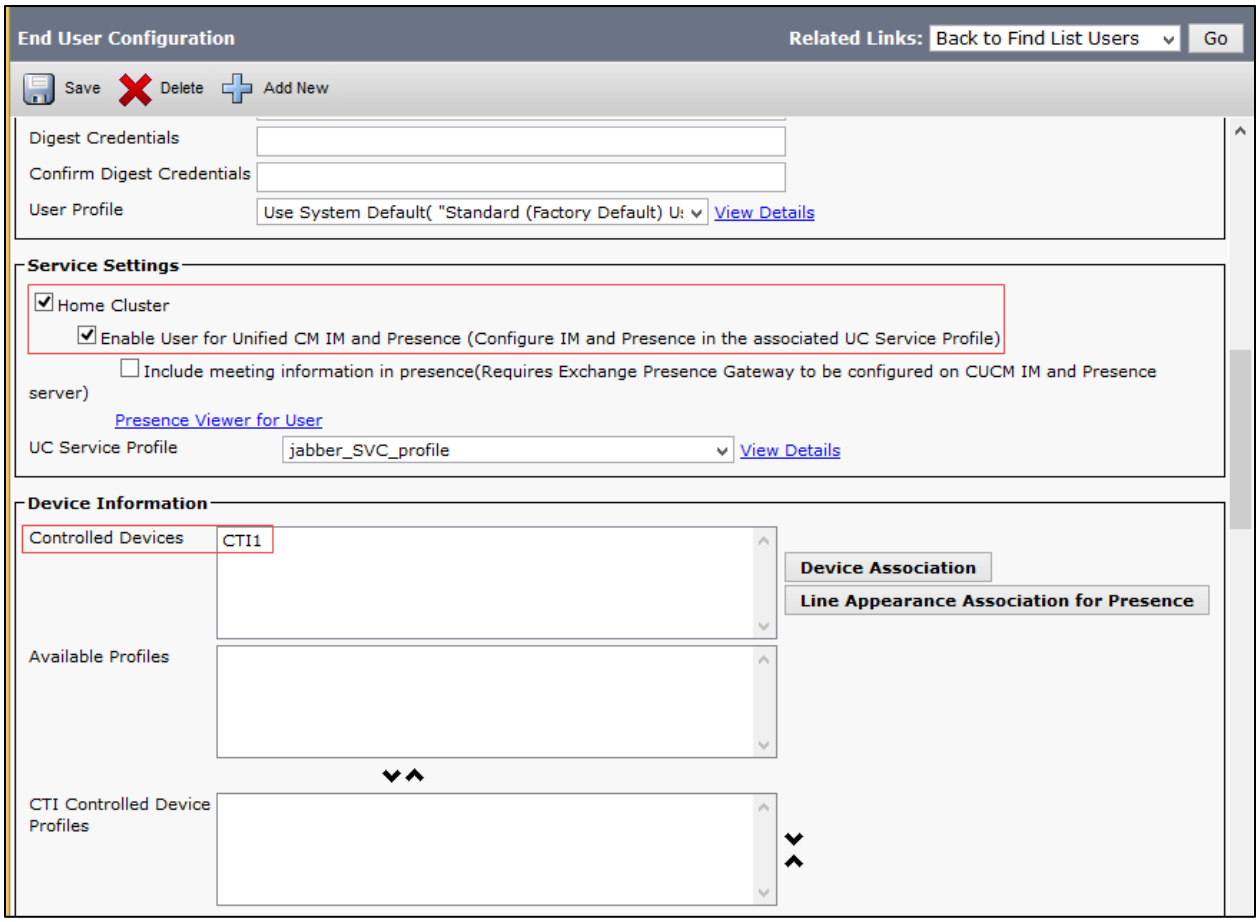
Check Home Cluster.

Click the Device Association

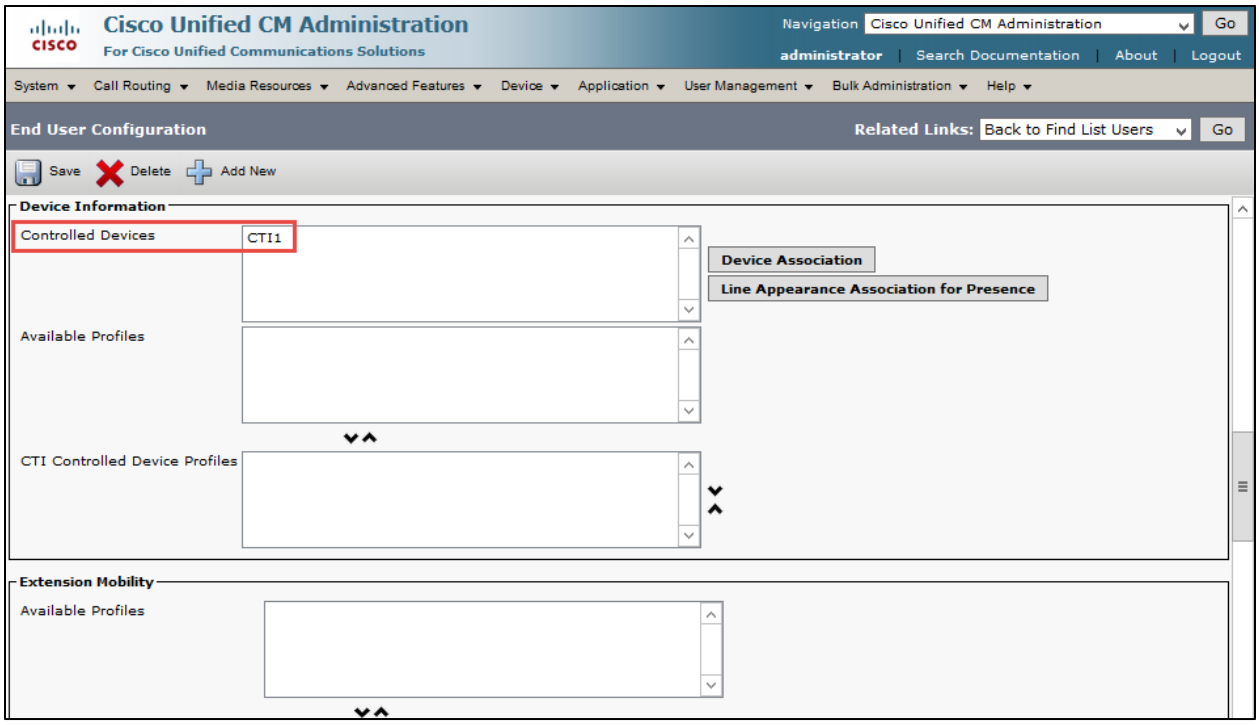
Select CTI1 from User Device Association screen



Cisco UCM end user Configuration (Continued)

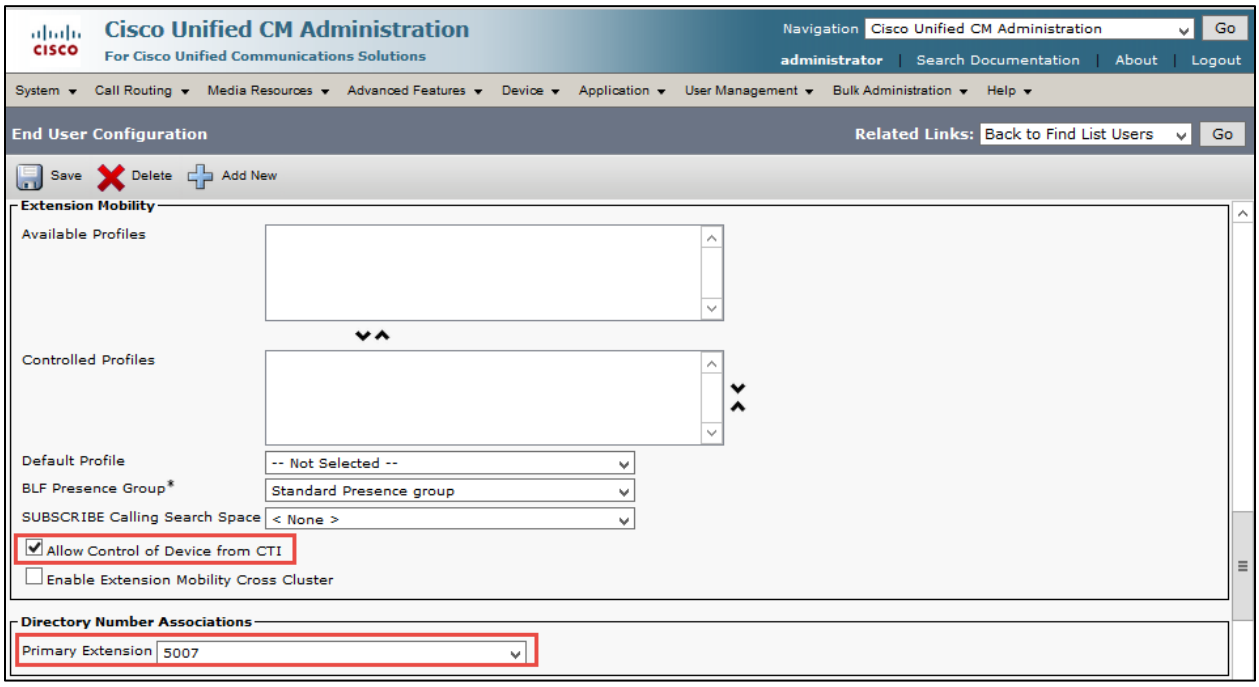


Cisco UCM end user Configuration (Continued)

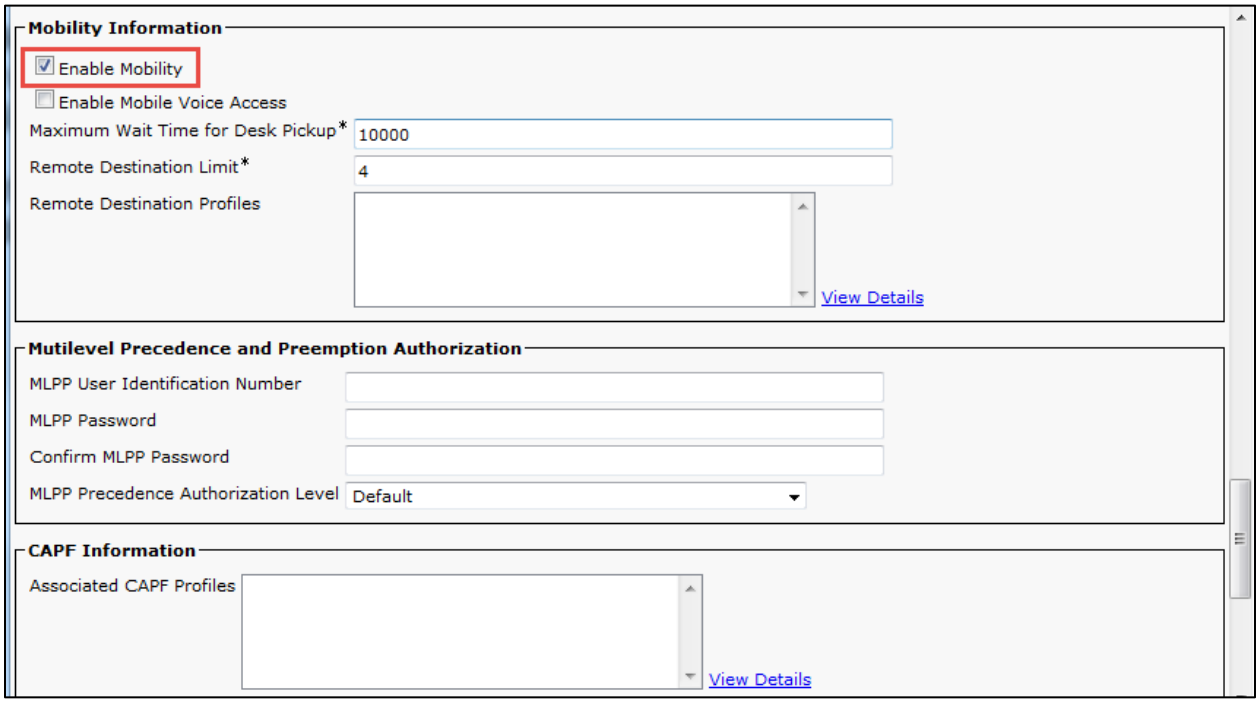


Cisco UCM end user Configuration (Continued)

Check Allow Control of Device from CTI
Select the Primary Extension for this user.5007 is used for this example.



Check Enable Mobility

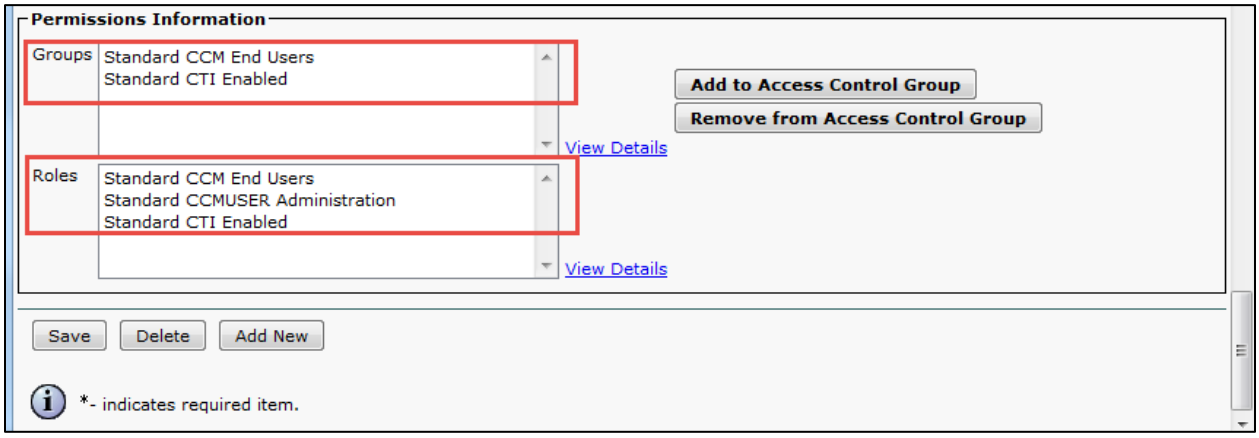


Add the following permissions for Standard Users:

–Standard CCM End-Users

–Standard CTI Enabled

–Standard CCMUSER Administration



Remote Destination Configuration

Navigation: Device→Remote Destination

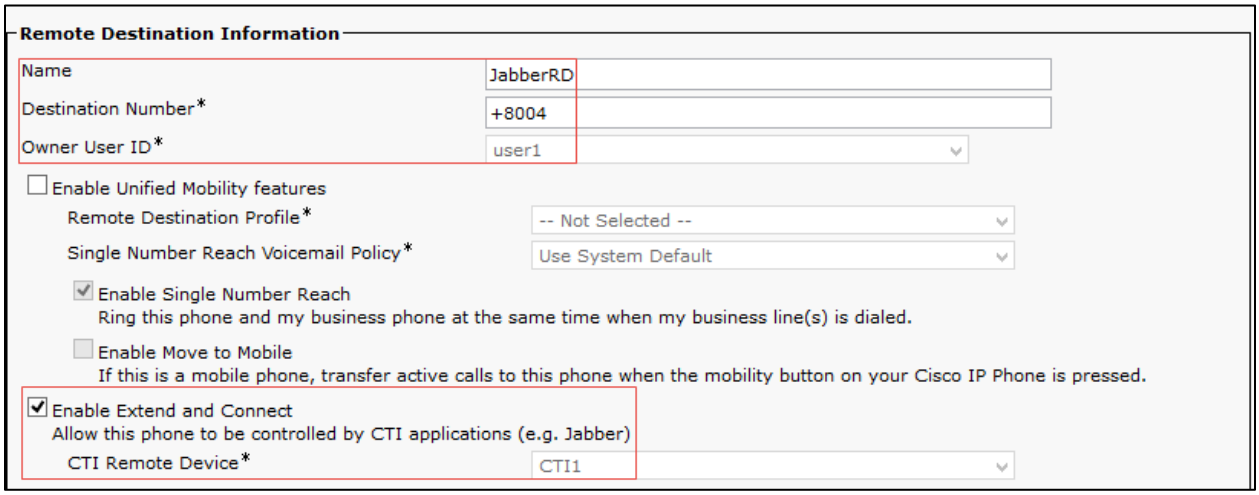
Add New

Set name = Jabber RD .This is used for the test

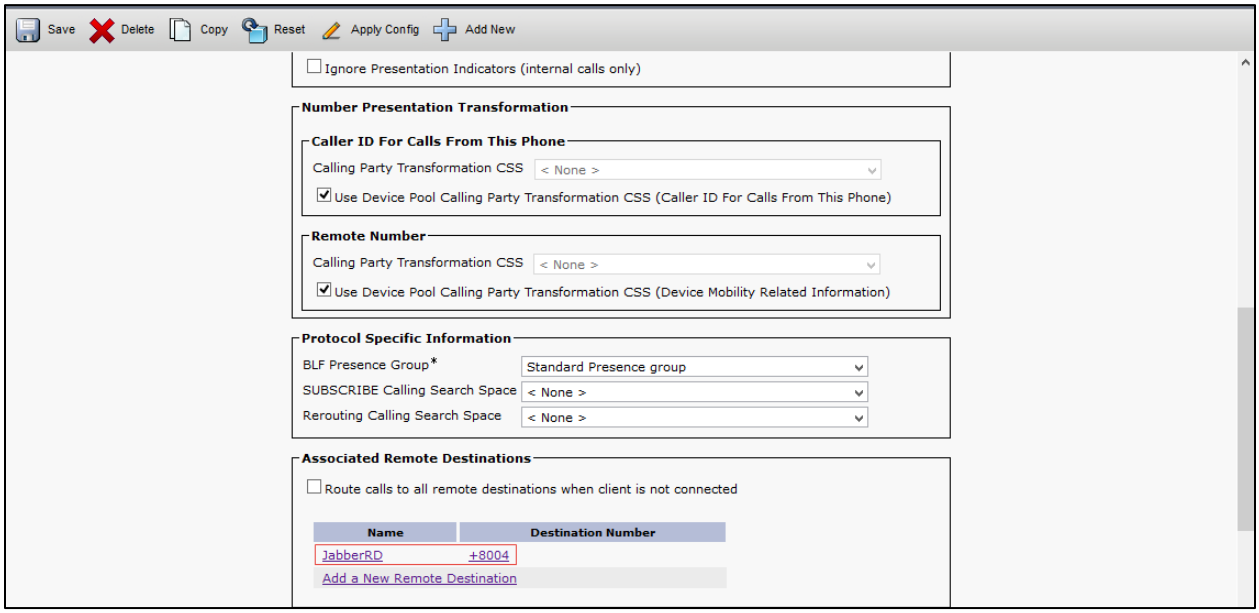
Set Destination Number*= +8004. This is used for the test. [8004 is a Skype for Business extension]

Check Enable Extend and Connect.

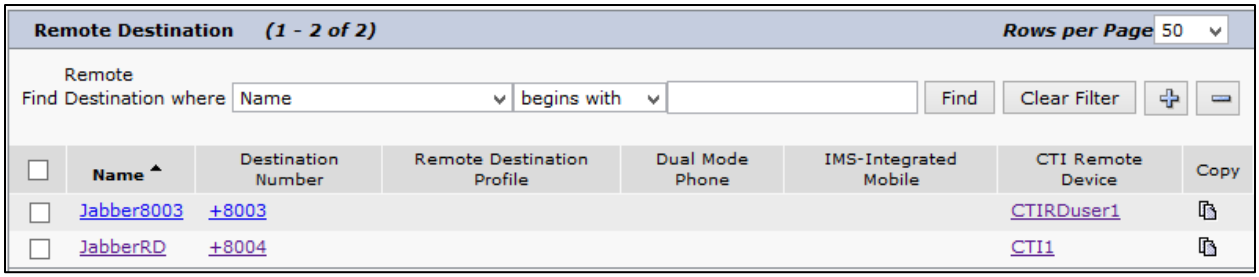
Set CTI Remote Device = CTI1



The CTI Remote Device configuration is updated with the remote destination:



Two Remote Destinations were configured for this test:



Cisco UCM CTI Remote Device Configuration

Navigation: Device→ Phone

Add New.

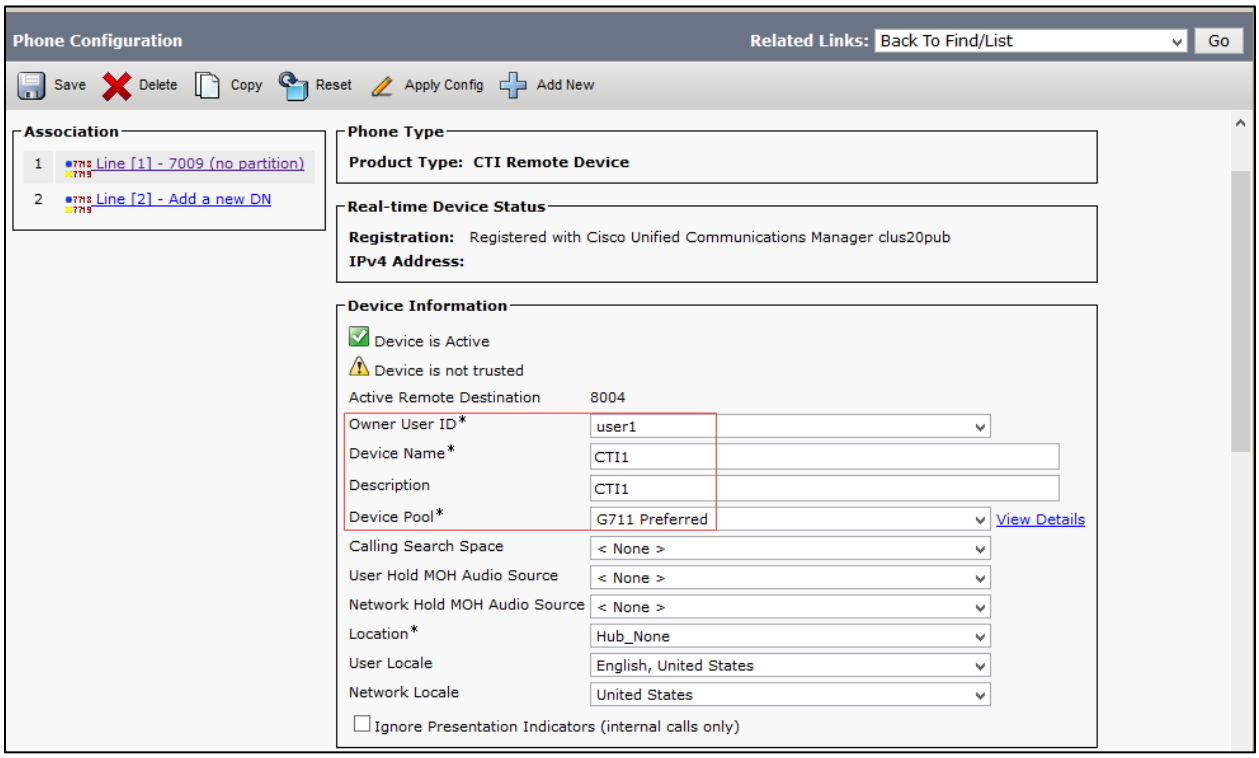
Select Phone Type * = CTI Remote Device

The CTI Remote Device type represents the user's remote device(s).

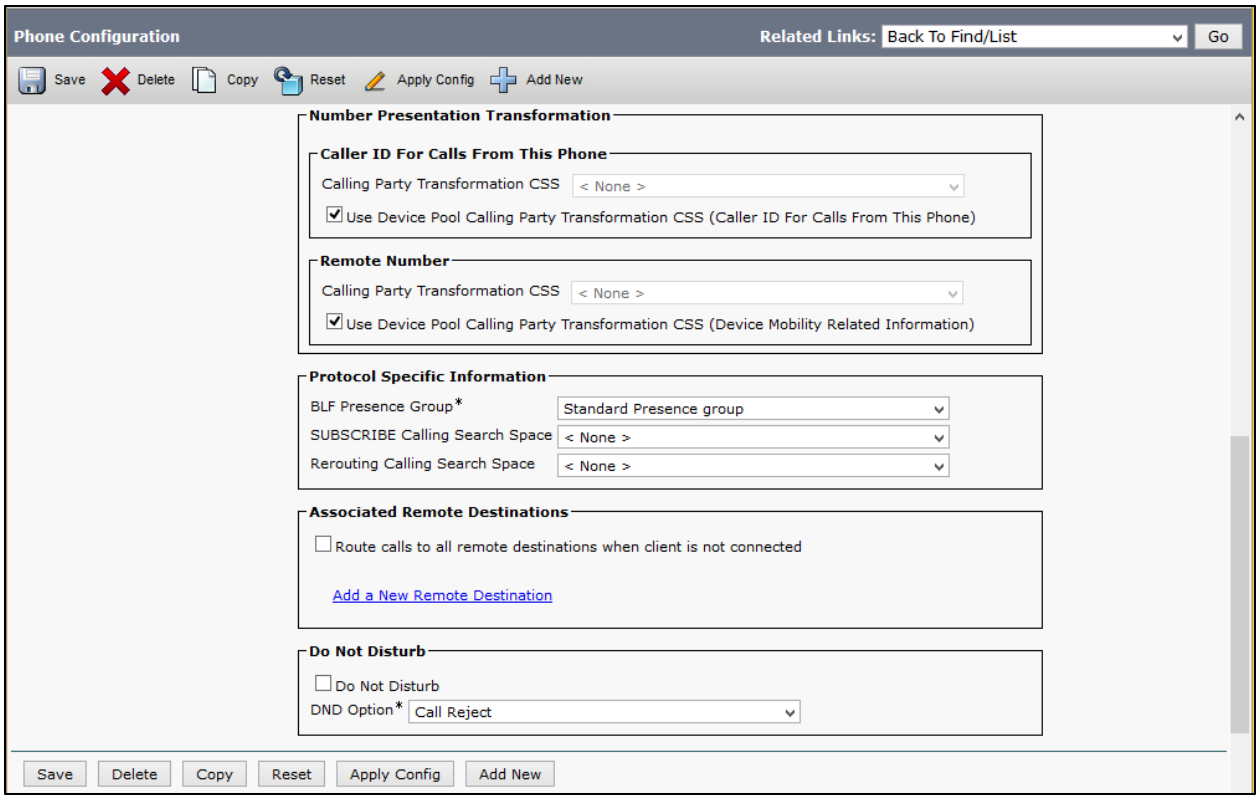
Select the desired Owner User ID. user1 is used in this test.

Set Device Pool: G711 Preferred

Save.



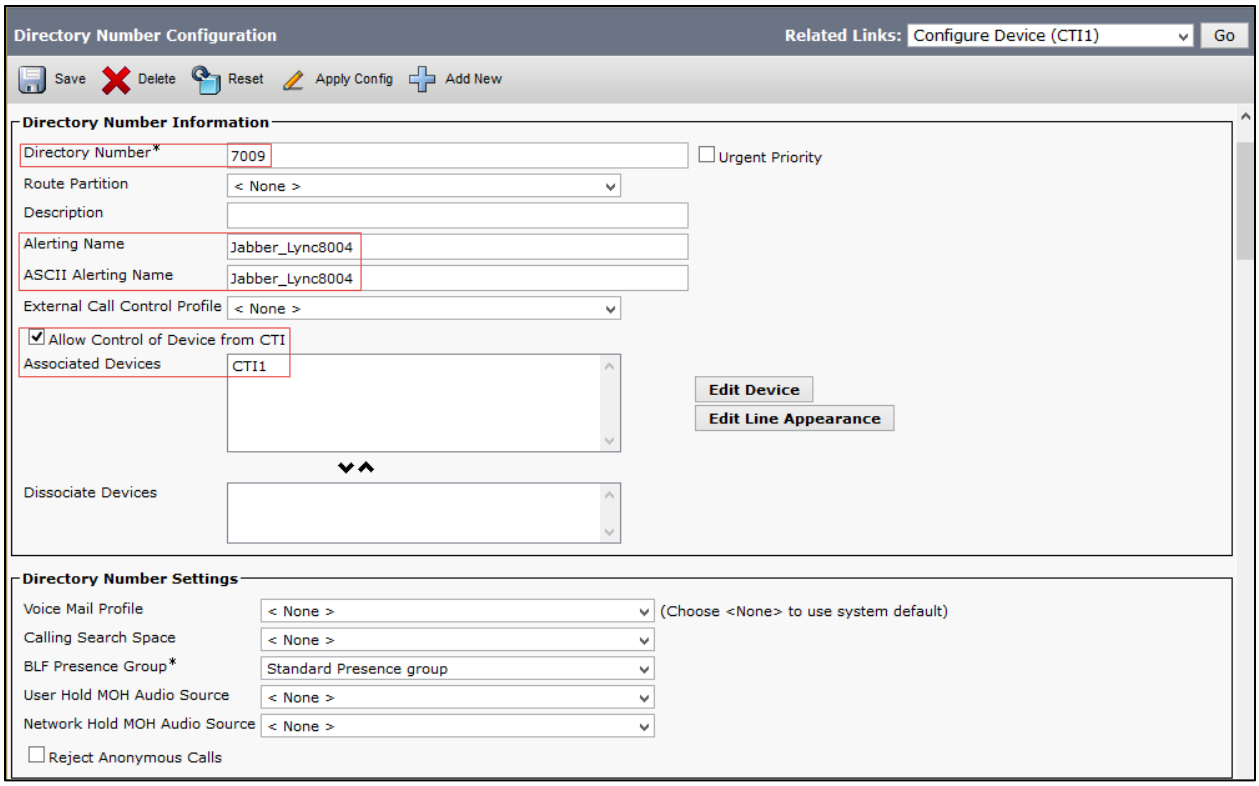
Cisco UCM CTI Remote Device Configuration (Continued)



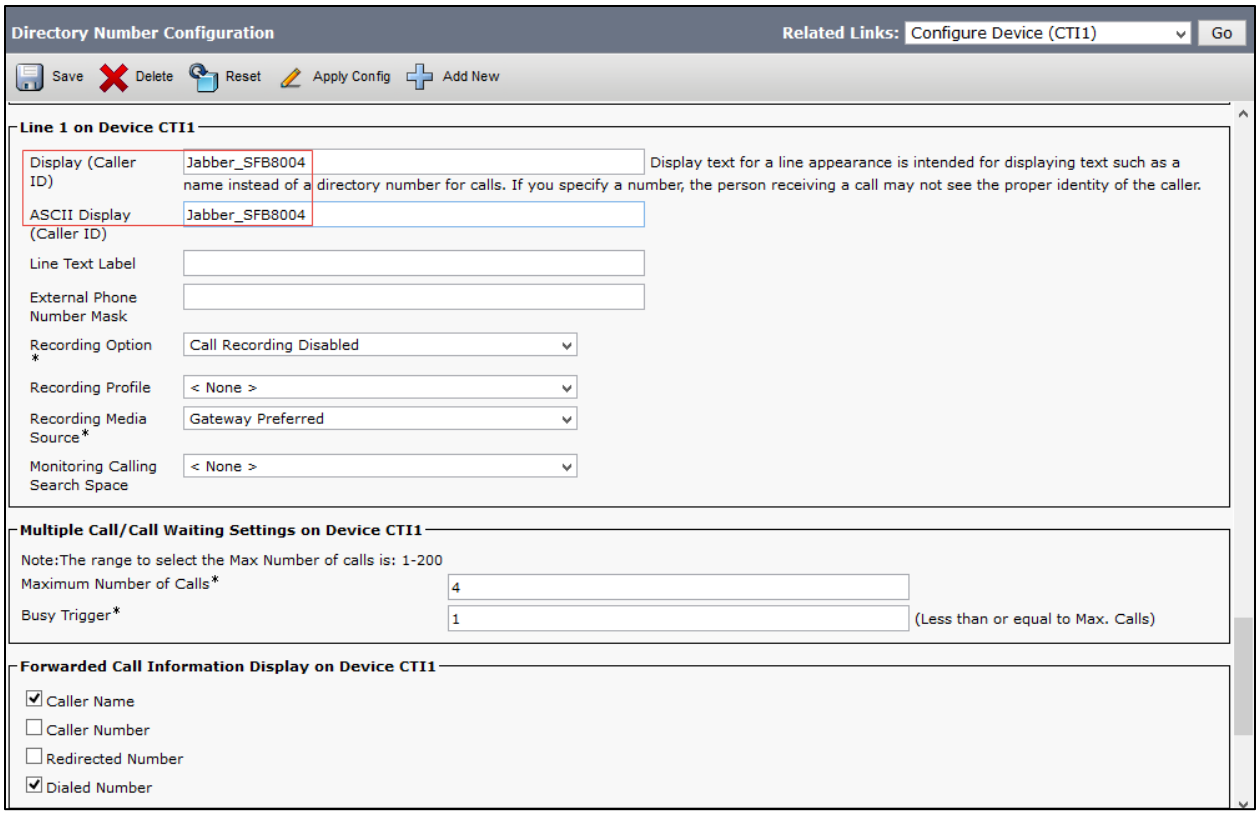
Add a DN to this device.

DN 7009 was configured for this test.

Cisco UCM CTI Remote Device DN Configuration



Cisco UCM CTI Remote Device DN Configuration (Continued)



Cisco Unity Connection

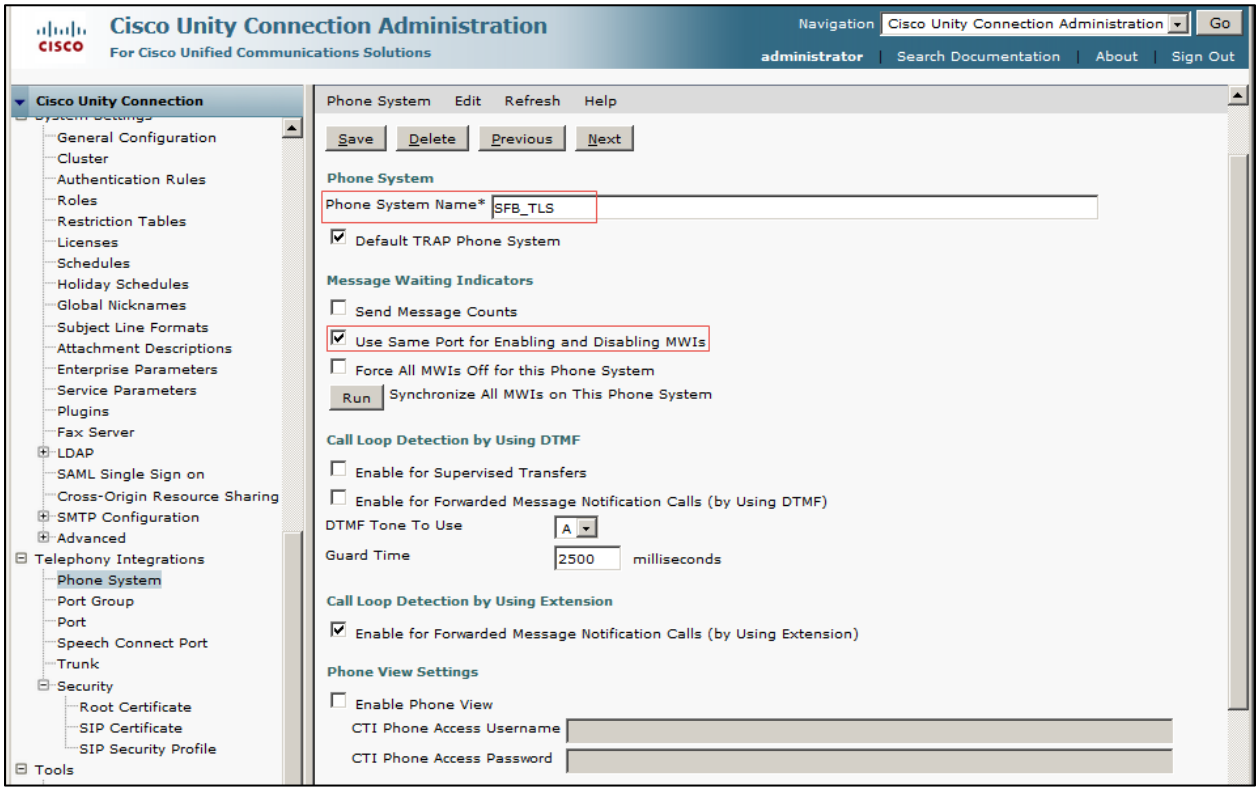
Cisco Unity Connection Telephony Integration – Add Phone System

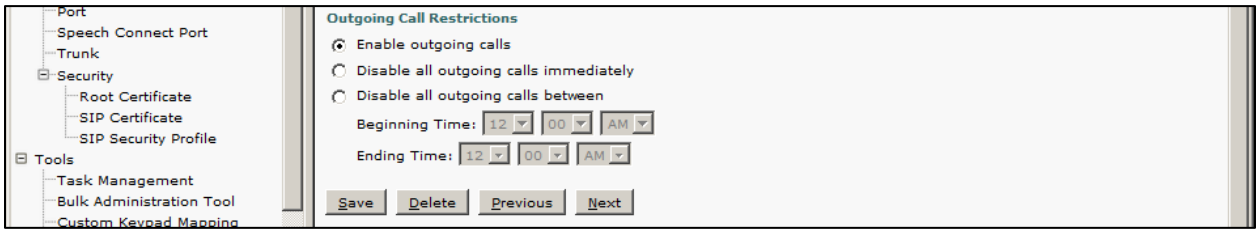
Navigation: Telephony Integrations → Phone system

Add New

Set Phone System Name* = SFB_TLS. This Name used for this test

Check Use Same Port for Enabling and Disabling MWIs





Cisco Unity Connection Telephony Integration – Add Port Group

Navigation: Telephony Integration → Port Group or from previous Screen, Related Links "Add Port Group" Go

Set Phone System = SFB_TLS

Set Create From – Port group Type = SIP

Set Display Name* = SFB_TLS-1.This Name used for this example.

Set Ipv4 Address or Host Name = 10.80.10.2 [This is the Cisco UCM publisher IP]

Check Register with SIP server

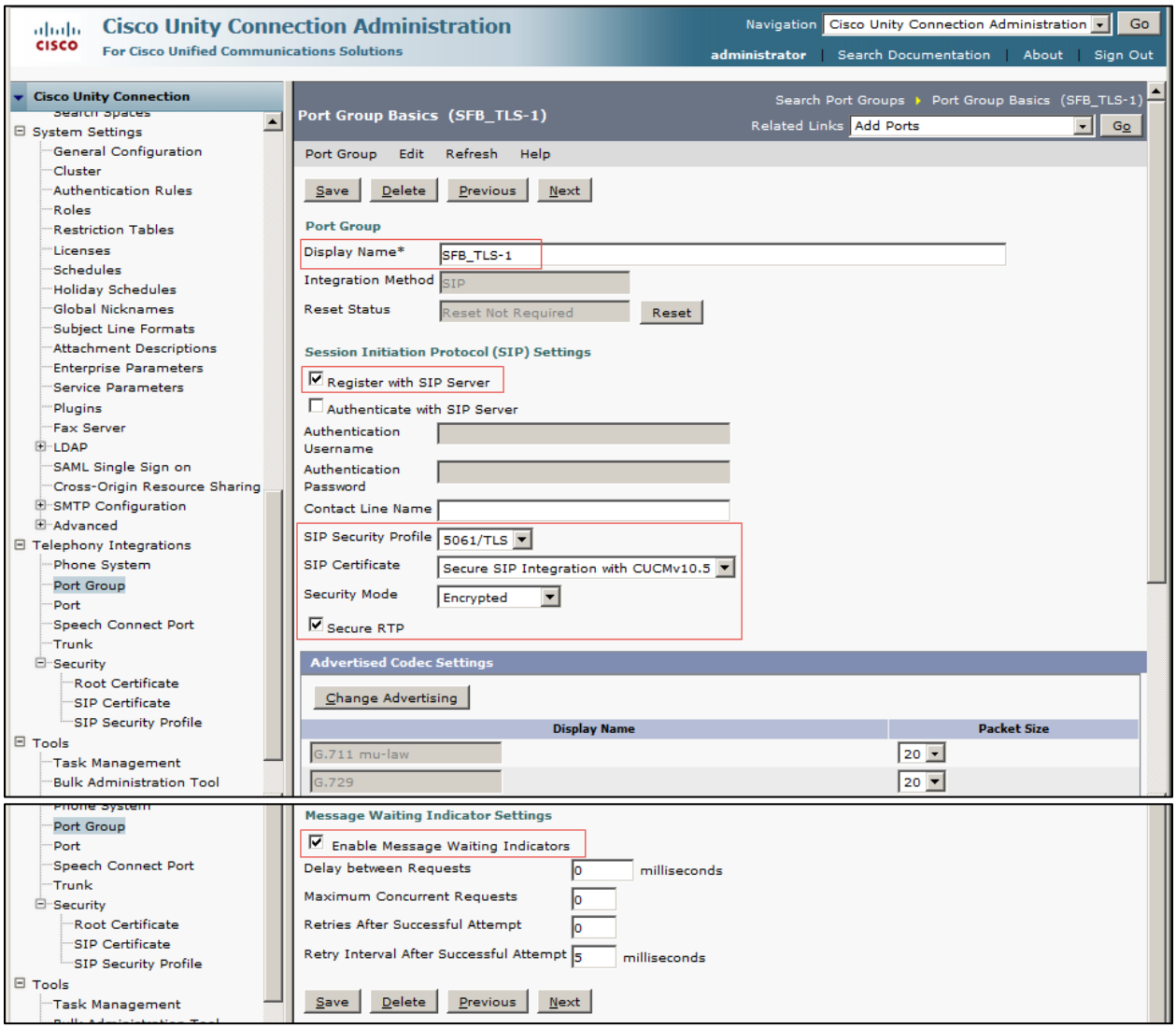
Set Security Profile = 5061/TLS

SIP Certificate = Secure SIP Integration with CUCMv10.5 (which is the display name of SIP Certificate generated in CUC under Security)

Set Security Mode = Encrypted

Check Secure RTP

Check Enable Message Waiting Indicators



Click Save.

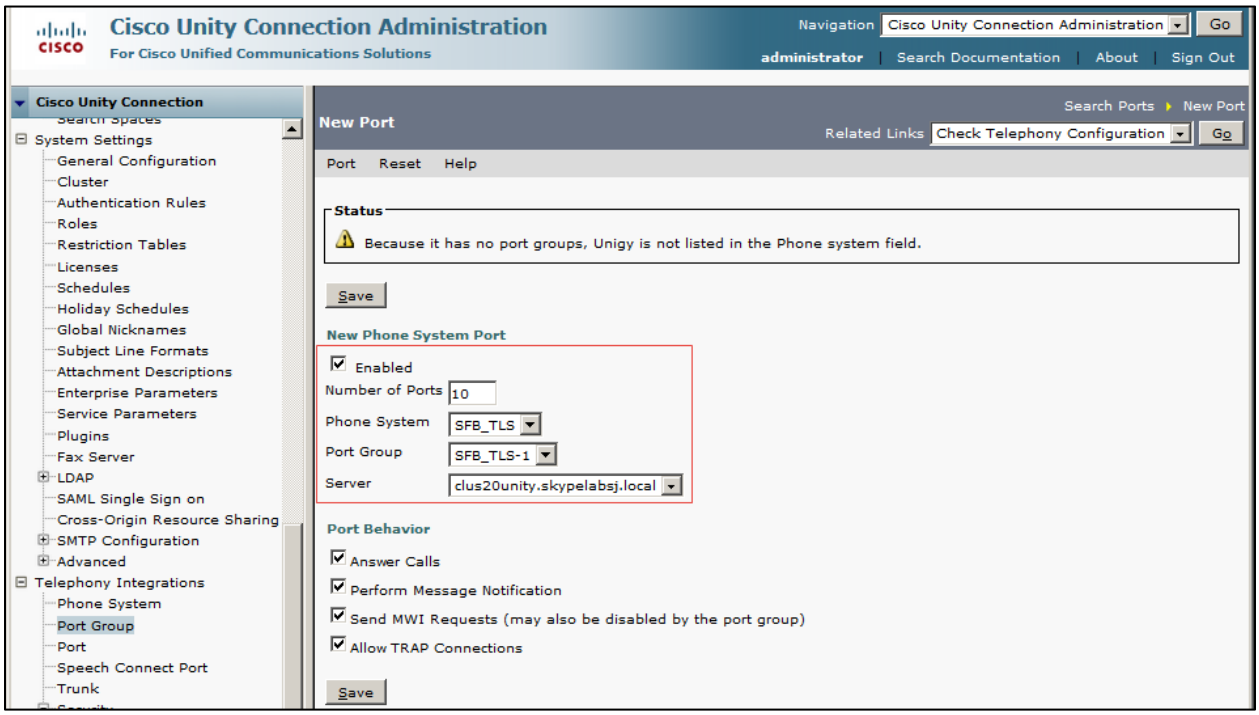
Cisco Unity Connection Telephony Integration – Add Ports

Set Number of Ports = 10

Set Phone System = SFB_TLS

Set Port Group = SFB_TLS-1

Set Server = clus20unity.skypelabsj.local (which is the FQDN of Cisco Unity Server)



Cisco Unity Connection User Configuration

Navigation: Cisco Unity Connection → Users → Users

Set Alias*= 8004 (This is used for the test)

Set First Name = User 1 (This is used to identify the User)

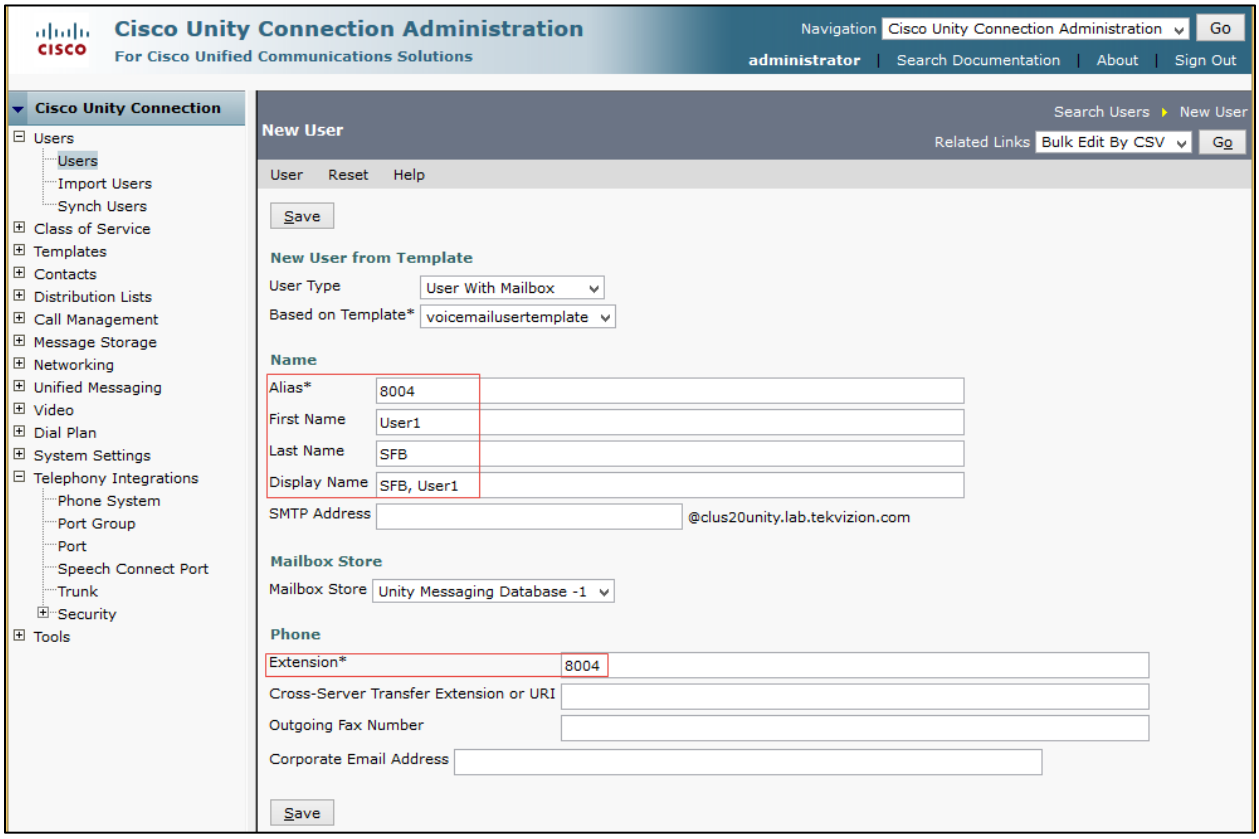
Set Last Name = SFB

Set Extension* = 8004 (This is user's extension number)

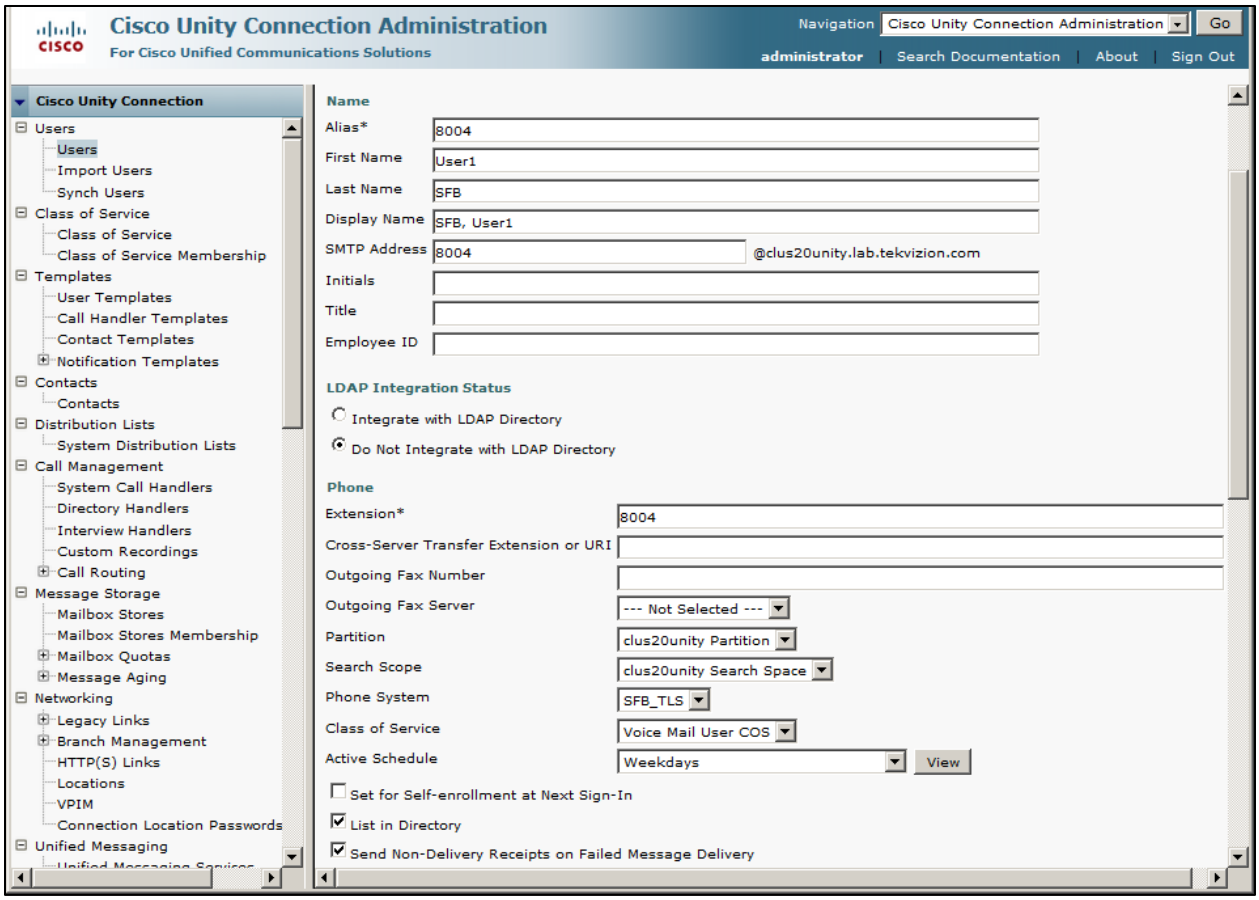
Save.

Set Phone System = SFB_TLS

Cisco Unity Connection User Configuration (Continued)

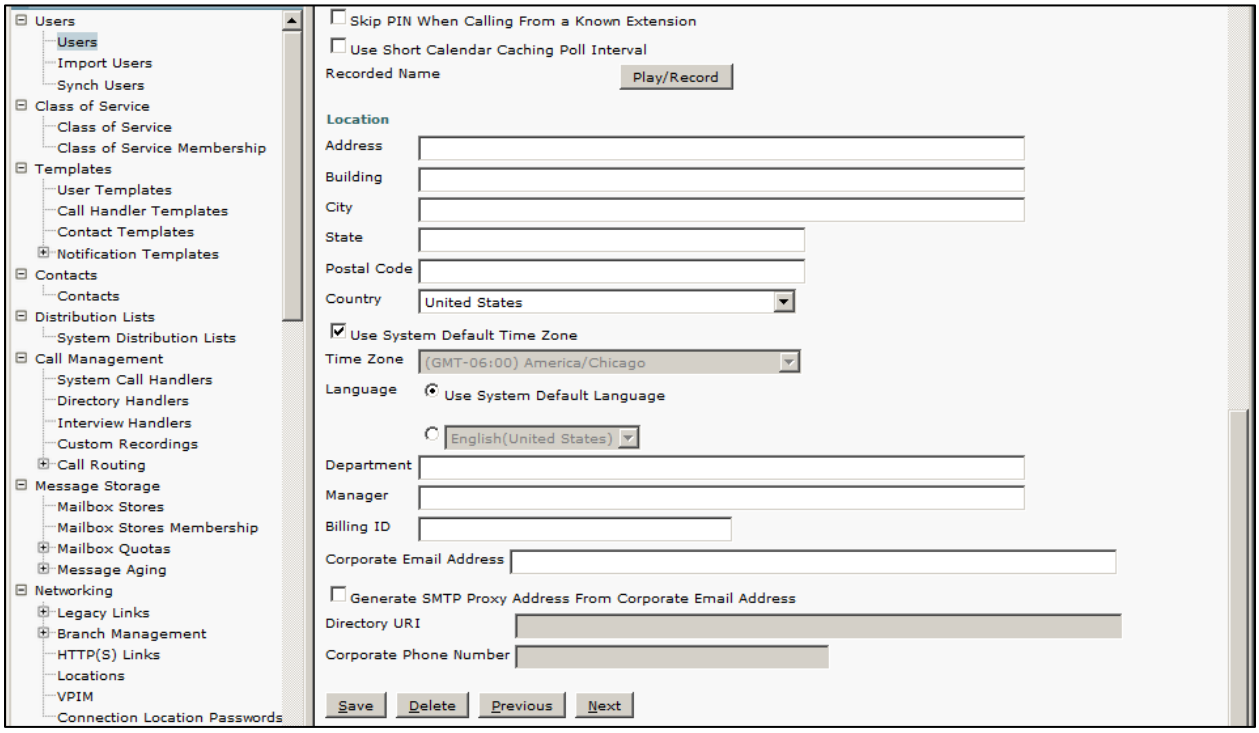


Cisco Unity Connection User Configuration (Continued)



Cisco Unity Connection User Configuration (Continued)

All values are default.



Similarly, create a user that has a Cisco extension.

Acronyms

Acronym	Definition
CCNR	Call Completion on No Reply
CFB	Call Forwarding on Busy
CFNA	Call Forwarding No Answer
CFU	Call Forwarding Unconditional
Cisco UCM	Cisco Unified Communications Manager
CLIP	Calling Line (Number) Identification Presentation
CLIR	Calling Line (Number) Identification Restriction
CNIP	Calling Name Identification Presentation
CNIR	Calling Name Identification Restriction
COLP	Connected Line (Number) Identification Presentation
COLR	Connected Line (Number) Identification Restriction
CONP	Connected Name Identification Presentation
CONR	Connected Name Identification Restriction
CT	Call Transfer
CUP	Cisco Unified Presence
DNS	Domain Name Server
EXT	Extension
FQDN	Fully Qualified Domain Name
MRGL	Media Resource Group List
MTP	Media Termination Point
MWI	Message Waiting Indicator
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
SCCP	Skinny Client Control Protocol
SFB	Skype for Business
SIP	Session Initiated Protocol
UDP	Uniform Dial Plan
VM	Voice Mail